T-Com

Teledat Router 800
Bedienungsanleitung

Sicherheitshinweise

Beachten Sie beim Aufstellen, Anschließen und Bedienen des Teledat Routers unbedingt die folgenden Hinweise:

- Bei Auf-Tisch-Betrieb: Stellen Sie das Gerät auf eine rutschfeste Unterlage!
- Achten Sie darauf, dass die Lüftungsschlitze nie verdeckt werden!
- Bei Wandmontage: Achten Sie darauf, dass Sie beim Bohren der Dübellöcher keine in der Wand befindlichen Leitungen oder Rohre treffen.
- Verlegen Sie die Anschlussschnüre unfallsicher!
- Wählen Sie den Aufstellungsort des Gerätes entfernt von:
  - Wärmequellen
  - direkter Sonneneinstrahlung
  - anderen elektrischen Geräten
- Schützen Sie das Gerät vor Nässe, Staub, Flüssigkeiten und Dämpfen.
- Schließen Sie die Anschlussschnüre nur an den dafür vorgesehenen Dosen an.
- Niemals
  - das Gerät selbst öffnen!
  - Steckkontakte mit spitzen und metallischen Gegenständen berühren!
- Reinigen Sie das Gerät mit einem weichen leicht feuchten Tuch. Reinigungsmittel oder Lösungsmittel sind nicht geeignet.
- Benutzen Sie das Gerät nicht in Feuchträumen (zum Beispiel Bad) oder in explosionsgefährdeten Bereichen.
- Den Teledat Router nur mit dem mitgelieferten Steckernetzgerät betreiben. Das Steckernetzgerät nicht mit nassen Händen anfassen. Nur an Stromsteckdosen anschließen, die den im Typenschild angegebenen Werten entsprechen.
- Das Gerät darf nur vom autorisierten Service-Personal repariert werden.
- **Eine Haftung der Deutschen Telekom für Schäden aus nicht bestimmungsgemäßem Gebrauch des Teledat Routers kann nicht übernommen werden.**

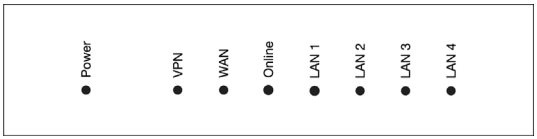
Für einen sorglosen Umgang mit Ihrem Produkt raten wir Ihnen, sämtliche Sicherheitseinstellungen (zum Beispiel Firewall, Verschlüsselung, Änderung Kennwort) vorzunehmen, die nicht bereits zum Zeitpunkt des Kaufs des Produkts aktiviert waren. Zusätzlich bitten wir Sie wegen der ständigen Änderungen – auch technischer Art - im Internet sowie technischer Weiterentwicklungen, sich zur Wahrung der sowohl zum Zeitpunkt des Kaufs bereits aktivierten als auch der durch Sie selbst veranlassten Sicherheitseinstellungen regelmäßig über aktuelle Hinweise zu Ihrem Produkt auf unserer Internet-Site www.telekom.de/teledatrouter800 zu informieren und ggf. neue Software-Versionen herunterzuladen.

Gesamtansicht: Vorderseite

Die nebenstehende Abbildung zeigt die **Vorderseite** Ihres Teledat Routers.

Hier befinden sich die Leuchtdioden.

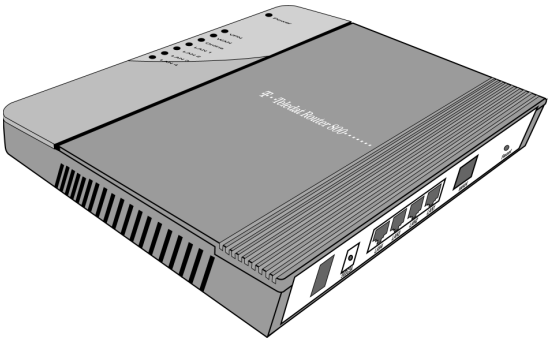
Leuchtdioden



Nebenstehende Abbildung zeigt die **Leuchtdioden** (LED), mit denen Ihr Teledat Router ausgestattet ist. In der nachfolgenden Tabelle wird deren Bedeutung im Einzelnen erklärt.

LED	Beschreibung
Power	Leuchtet, wenn das Gerät eingeschaltet und betriebsbereit ist.
VPN	Leuchtet, wenn eine VPN-Verbindung aufgebaut ist.
WAN	Leuchtet, wenn eine Verbindung zum DSL-Modem besteht.
Online	Leuchtet, wenn eine DSL-/Breitbandverbindung zum ISP besteht.
LAN1 bis LAN4	Leuchtet orange bei einer 10 MBit-Verbindung und grün bei einer 100 MBit-Verbindung.

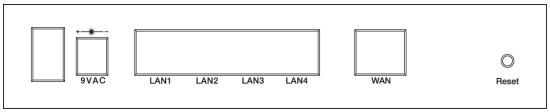
Gesamtansicht: Rückseite



Auf diesem Bild sehen Sie die **Rückseite** Ihres Teledat Routers.

Hier befinden sich die Anschlüsse unter anderem für Strom, LAN und WAN.

Anschlüsse



Nebenstehende Abbildung zeigt die **Anschlüsse** Ihres Teledat Routers.
In der nachfolgenden Tabelle wird deren Bedeutung im Einzelnen erklärt.

Anschluss	Beschreibung
	Ein- / Ausschalter
9 VAC	Buchse zum Anschluss des Steckernetzgerätes
LAN1 bis LAN4	LAN-Anschlüsse (Ethernet): kann sowohl als Patch- und als Uplinkport verwendet werden.
WAN	WAN-Anschluss (Verbindung zum DSL-Modem)
Reset	Reset-Taste: setzt den Router auf Werkseinstellungen zurück, wenn er im laufenden Betrieb etwa fünf Sekunden gedrückt wird.

Inhaltsverzeichnis

Einleitung 4

Eigenschaften des Teledat Routers 800....4
Grundfunktionen des Teledat Routers 800....4

Inbetriebnahme 6

Lieferumfang....6
Systemvoraussetzungen....7
Aufstellungsort....7
Auf-Tisch-Betrieb....7
Wandmontage....7
Hardwareinstallation....8
Anschließen an das Stromnetz....8
DSL-Anschluss....8
LAN-Anschluss....9
Einbindung in das LAN....9
Vorbereitung des einzubindenden Rechners / Netzwerkes....9
Computer mit Windows 95/98/Me einrichten....10
Computer mit Windows NT/2000/XP einrichten....11
Erstkonfiguration des Teledat Routers 800....12
Der Web-Konfigurator....12
Erstes Login....14
Erstkonfiguration mit dem Assistenten....15

Teledat Router 800 konfigurieren 16

Login....16
Home....17
Assistent....18
Basiskonfiguration....18
Passwort....18
Systemzeit....19
LAN / DHCP / DNS....20

Internetzugang....22
PPPoE / T-DSL....22
PPTP....24
Standleitung....26
Budgetkontrolle....27
Status....27
Konfiguration....28
Firewall / NAT....31
Grundeinstellungen....31
IP-Filter....32
DoS-Abwehr....35
Portumleitung....37
Portöffnung....40
DMZ....42
VPN / Routing....43
Zugangskontrolle....43
Entfernte Nutzer....44
PPP Protokoll....45
VPN Profile....46
IKE / IPSec-Schlüssel....52
Static Route....53
Extras....54
Dynamisches DNS....54
Verbindungstimer....56
Verwaltung....57
Einstellungen....57
SysLog....58
Konfig. sichern....59
Firmwareupgrade....60
Neustart....62
Status....62
VPN-Status....62
Anwahlpaket....63
Routingtabelle....64
Portumleitungen....64
ARP Cache....65

DHCP Daten ... 65
NAT Adresstabelle ... 66

Anwendungen mit dem Teledat Router 800 **67**

LAN-LAN-Kopplung mit VPN über Internet ... 67
Unidirektionale LAN-LAN-Kopplung ... 67
Bidirektionale LAN-LAN-Kopplung ... 71
Bidirektionale LAN-LAN-Kopplung mit IPSec-Verschlüsslung ... 74
Entfernte Nutzer einbinden ... 78
Nutzerprofil definieren ... 78
Benutzereinwahl über Windows XP ... 80

Anhang **82**

Routertools für Microsoft Windows ... 82
Installation der Routertools ... 82
Teledat Firmware Upgrade ... 83
Teledat Syslog ... 84
Erste Hilfe ... 86
Service / Support ... 88
CE-Zeichen ... 88
Technische Daten ... 89
Gewährleistung ... 90
Reinigen ... 91
Recycling ... 91
Stichwortverzeichnis ... 92
Glossar ... 95

Einleitung

Dieses Kapitel gibt Ihnen zunächst einen Überblick über die wichtigsten Funktionen und Anwendungen Ihres Teledat Routers 800.

Eigenschaften des Teledat Routers 800

Ihr Teledat Router 800 ist ein Gateway für Ethernet-Netzwerke, das Ihren Rechnern den Zugang zum Internet über DSL ermöglicht. Er zeichnet sich durch eine große Funktionsvielfalt bei einfacher Konfiguration aus.

Grundfunktionen des Teledat Routers 800

Integrierter Switch mit vier Netzwerkanschlüssen

Dank der Kombination von Router und Switch in einem Gerät ist der Teledat Router 800 eine kostengünstige und leistungsstarke Netzwerklösung. Sie können bis zu vier Computer direkt an das Gerät anschließen; für den Anschluss von mehr als vier Computern verwenden Sie zusätzlich einen externen Hub oder Switch.

10/100 Mbit/s-Ethernet-Anschlüsse mit automatischer Geschwindigkeitsanpassung

Die automatische Bandbreitenerkennung für 10 bzw.100 Mbit/s bietet einen verbesserten Datendurchsatz als herkömmliche Hubs, da die volle Bandbreite dediziert und nicht geteilt zur Verfügung gestellt wird. Die automatische Anpassung der Übertragungsgeschwindigkeit sorgt dafür, dass empfangene Daten problemlos und ohne Benutzereingriff übermittelt werden können. Das Gerät unterstützt Geschwindigkeiten von 10 bzw.100 Mbit/s im Halb-und Vollduplexbetrieb und passt sich so problemlos an Ihr Ethernet-Netzwerk an. Außerdem erkennt der Teledat Router an jedem seiner LAN-Anschlüsse automatisch, ob dort ein Computer als Endgerät oder ein Hub bzw. Switch als Verteiler angeschlossen ist. Er passt sich automatisch daran an. Ihnen bleibt auf diese Weise die Verwendung spezieller Verbindungskabel erspart – alle Netzwerkgeräte lassen sich über einfache „straight-through“ - Kabel anschließen.

Vollständige Netzwerkverwaltung per Web-Browser

Die Konfiguration des Teledat Routers ist durch die Bedienung per Web-Browser und mit der Unterstützung durch die integrierte Hilfe besonders übersichtlich und einfach.

Budget-Kontrollmöglichkeit

Kontrollieren Sie automatisch Verbindungszeit und Datentransfervolumen mit der Budget-Kontrolle. Dabei können Sie für einen Monat bestimmte Zeit-und Volumenkontingente festlegen. Werden diese erreicht, sperrt der Router auf Wunsch den Internet-Zugang. Die aktuellen Verbrauchswerte können Sie jederzeit über den Web-Konfigurator abrufen.

NAT (Network Address Translation)

Die NAT-Funktion (Network Address Translation) ermöglicht es mehreren Rechnern in einem Netzwerk die gleiche externe IP-Adresse zu benutzen. Für den Betrieb von internen Diensten wie Web- oder Fileserver ist die Umleitung von öffentlichen Ports auf bestimmte interne Rechner mit den Features Portumleitung, Portöffnung und DMZ-Server möglich.

DHCP-Unterstützung

DHCP (Dynamic Host Configuration Protocol) ermöglicht es den Clients, beim Anmelden an das Netzwerk automatisch die TCP/IP-Einstellungen von einem zentralen DHCP-Server zu beziehen. So weist das Gerät automatisch eine IP-Adresse zu und übermittelt die IP-Adresse des Standard-Gateways an alle Computer, die die DHCP-Client-Funktion unterstützen. Bei Bezug einer IP-Adresse vom Server Ihres Providers verhält sich der Teledat Router wie ein DHCP-Client.

VPN (Virtuelles Privates Netzwerk)

Der Teledat Router integriert VPN-Server und Client. Neben PPTP unterstützt er auch VPN-Verbindungen über IPSec und L2TP, mit und ohne DES-Verschlüsselung. Es können bis zu 8 VPN-Verbindungen gleichzeitig aufgebaut werden. Der VPN-Tunnel kann zwischen zwei Routern oder zwischen Router und PC mit kompatibler Software aufgebaut werden.

Konfigurierbare Firewall

Das Internet wird physikalisch von Ihrem lokalen Hausnetz (Intranet) getrennt. Dazu verfügt Ihr Router über separate Ethernetanschlüsse für Internet und Intranet. Diese Anschlüsse sind durch eine konfigurierbare Firewall getrennt. Im Ergebnis werden nur Datenpakete zwischen den Netzen ausgetauscht, die vorher zugelassen wurden. Unerwünschte Übertragungen werden automatisch abgeblockt.

Datum und Uhrzeit

Beim Verbinden mit dem Internet bezieht der Teledat Router das aktuelle Datum und die exakte Uhrzeit von einem Zeitserver im Internet. Dadurch kann das Gerät eine sekundengenaue Protokollierung aller Vorgänge gewährleisten.

Protokolle

Die Protokollierungsfunktion (SysLog) ist konfigurierbar. Sie können einstellen, welche Vorgänge für Sie von Bedeutung sind und protokolliert werden sollen.

Status

Informationen zum aktuellen Zustand des Routers, zum Beispiel Routingtabellen, DHCP-Daten oder Portumleitungen etc. finden Sie in den umfassenden Statusseiten des Web-Konfigurators.

Inbetriebnahme

Ihr Teledat Router ist ein hochwertiges Gerät, das zu Ihrer Zufriedenheit arbeitet, wenn Sie die für die Inbetriebnahme notwendigen Voraussetzungen beachten.

Lieferumfang

Der Lieferumfang Ihres Teledat Routers umfaßt:

- Teledat Router 800
- 230V Steckernetzgerät für deutsche Steckdosen
- zwei Kabel RJ-45
- CD-ROM mit Software
- Kurzanleitung zur Installation Ihres Teledat Routers
- Ausführliche gedruckte Bedienungsanleitung

Bevor Sie Ihren Teledat Router in Betrieb nehmen, sollten Sie zunächst sorgfältig überprüfen, ob irgendwelche Schäden

- am **Gehäuse**
- am **Steckernetzgerät** beziehungsweise **Netzkabel** sichtbar sind.

Auf keinen Fall dürfen Sie das Gerät in Betrieb nehmen, wenn Sie Beschädigungen feststellen! Wenden Sie sich im Zweifelsfall an unseren Service unter der Rufnummer 0180 5 1990. Der Vebindungspreis beträgt 0,12 EUR pro angefangene 60 Sekunden bei einem Anruf aus dem Festnetz der Deutschen Telekom (Stand Mai/2003).

Tipp

Heben Sie die Originalverpackung auf. Sie können Sie dann für einen Transport oder zum Versand verwenden.

Systemvoraussetzungen

Für den Einsatz Ihres Teledat Routers sollten folgende Voraussetzungen erfüllt sein:

- T-DSL-Anschluss und T-DSL-Modem, zum Beispiel Teledat 330/331 LAN oder TCP/IP-basierenden WAN-Anschluss
- PCs mit Ethernetanschluss und TCP/IP-Unterstützung und beliebigem Betriebssystem

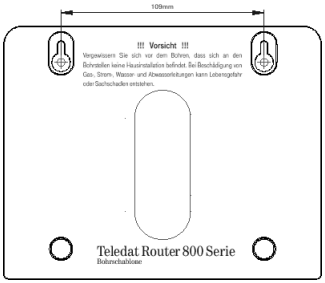
Aufstellungsort

Der Aufstellungsort des Teledat Routers muss sich in der Nähe einer Stromsteckdose befinden.

Auf-Tisch-Betrieb

Ihr Teledat Router ist für den Tischbetrieb vorgesehen. Die heutigen Möbel sind mit einer unübersehbaren Vielfalt an Lacken und Kunststoffen beschichtet und werden mit unterschiedlichen Lackpflegemitteln behandelt. Es ist nicht auszuschließen, dass manche dieser Stoffe Bestandteile enthalten, die die Kunststofffüße des Routers angreifen und aufweichen. Die so durch Fremdstoffe veränderten Gerätefüße können auf der Oberfläche der Möbel Spuren hinterlassen. Die Deutsche Telekom kann für derartige Schäden nicht haften.

Wandmontage


109mm
!!! Vorsicht !!!
Vergewissern Sie sich vor dem Bohren, dass sich an den Bohrstellen keine Hausinstallation befindet. Bei Beschädigung von Gas-, Strom-, Wasser- und Abwasserleitungen kann Lebensgefahr oder Sachschaden entstehen.
Teledat Router 800 Serie
Bohrschablone

Sie können Ihren Teledat Router auch an der Wand befestigen. Dafür sind an der Unterseite Bohrungen angebracht.

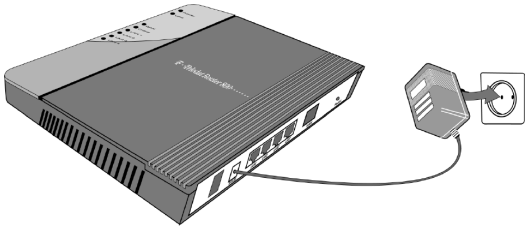
Achten Sie beim Befestigen darauf, dass die LEDs sichtbar bleiben und die Kabel nicht geknickt werden.

!

Beachten Sie beim Anbringen der Schrauben alle handwerklichen Vorsichtsmaßnahmen, zum Beispiel beim Bohren und Dübeln. Die Deutsche Telekom kann für entstehende Schäden nicht haften.

Hardwareinstallation

Anschließen an das Stromnetz



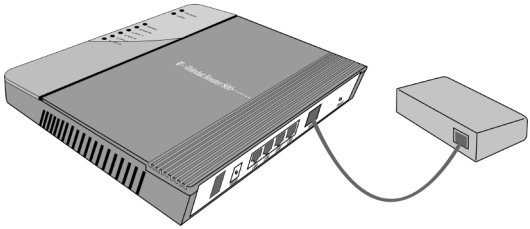
Für den Anschluss an das Stromnetz prüfen Sie, ob die Anschlusswerte der Stromsteckdose denen entsprechen, die für die Primärseite des Steckernetzgeräts auf dem Typenschild angegeben sind.

Stecken Sie den Stecker des dünnen Kabels in die Anschlussbuchse für das Steckernetzgerät im Teledat Router. Schließen Sie das Steckernetzgerät über eine eigene Steckdose an.

Stecken Sie das Steckernetzgerät nie in eine Steckdose, von der Sie nicht sicher sind, dass sie den auf dem Typenschild angegebenen Werten entspricht: Steckernetzgerät und Gerät können zerstört werden, Sie können körperlichen Schaden erleiden.

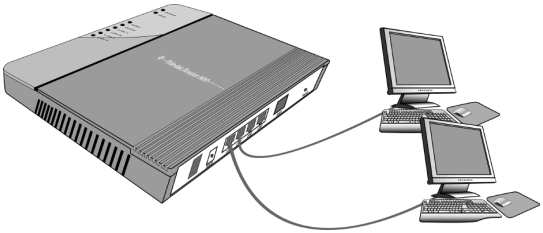
Schalten Sie nun den Router am Hauptschalter an der Rückseite des Gerätes ein. Jetzt leuchtet die grüne LED **Power** an der Vorderseite des Teledat Routers.

DSL-Anschluss



Mit einem der beiden mitgelieferten Kabel verbinden Sie den WAN-Port des Teledat Routers mit dem DSL-Modem. Wird das Modem korrekt erkannt, leuchtet die LED **WAN** und eine entsprechende LED am Modem.

LAN-Anschluss



Für den Anschluss an das lokale kabelgebunde Netz (LAN) stecken Sie das zweite im Lieferumfang enthaltene RJ-45 Kabel in eine der mit **LAN1** bis **LAN4** gekennzeichneten Buchsen an der Rückseite des Routers.

Das andere Ende stecken Sie in die Buchse der Ethernet-Schnittstelle an Ihrem Rechner. Auf diese Weise können Sie noch drei weitere Rechner direkt anschließen. Wird der Rechner erkannt, so leuchtet die entsprechende LED unter **LAN** auf. Haben Sie zum Beispiel Ihren Rechner mit dem Anschluss LAN1 an Ihrem Teledat Router verbunden, leuchtet die LED LAN1. Werden Daten übertragen, so blinkt diese Leuchtdiode. Beim Teledat Router leuchten die LEDs bei einer 10 MBit-Verbindung orange, bei einer 100 MBit-Verbindung grün.

Einbinden in das LAN

Sie benötigen keine spezielle Installationssoftware, um Ihren Teledat Router in Ihr lokales Netz einzubinden und um einen Zugang ins öffentliche Netz herzustellen.

Das Einbinden ins LAN geschieht mit den Hilfsmitteln, die das Betriebssystem (Windows® 98, 98SE, Me, 2000, XP) Ihres Rechners zur Verfügung stellt. Rechner mit anderen Betriebssystemen und mit TCP/IP-Unterstützung können grundsätzlich ebenfalls angeschlossen werden. Die Deutsche Telekom kann hierfür jedoch keine Funktionsgarantie und keine Unterstützung durch den Kundendienst geben.

Das Herstellen einer Verbindung ins Internet und das Konfigurieren von IP-Adressen geschieht mittels des Web-Konfigurators (HTML-basierter Assistent für das Konfigurieren der Zugangsdaten). Dieser Konfigurator ist in der Firmware des Teledat Routers enthalten. Über den von Ihnen verwendeten Internetbrowser (zum Beispiel Internet Explorer®, Netscape Navigator®, Opera®) können Sie den Konfigurator aufrufen.

Vorbereitung des einzubindenden Rechners / Netzwerkes

Sie haben den Anschluss Ihres Teledat Routers an Ihr lokales Netzwerk und an das DSL-Modem wie vorn beschrieben (siehe Seite 8) durchgeführt. Schalten Sie Ihren Router ein, sodass die LED **Power** leuchtet. Um eine Verbindung zu Ihrem Teledat Router aufbauen zu können, müssen Ihre Rechner eine passende TCP/IP-Konfiguration haben.

Die TCP/IP-Einstellungen sind für alle Betriebssysteme ähnlich. Für die gebräuchlichsten Betriebssysteme ist die Netzwerkkonfiguration im Folgenden beschrieben.

Computer mit Windows 95/98/Me einrichten

TCP/IP-Komponenten installieren

1. Klicken Sie auf „Start" – „Einstellungen" – „Systemsteuerung" und doppelklicken Sie im Fenster „Systemsteuerung" auf das Netzwerk–Symbol. Daraufhin werden im Fenster „Netzwerk" alle bereits eingerichteten Komponenten angezeigt.
2. Klicken Sie im Fenster „Netzwerk" auf die Schaltfläche „Hinzufügen".
3. Wählen Sie „Protokoll", und klicken Sie auf „Hinzufügen".
4. Wählen Sie aus der Herstellerliste den Eintrag „Microsoft".
5. Wählen Sie aus der Protokollliste den Eintrag „TCP/IP", und klicken Sie auf „OK".

TCP/IP einrichten

1. Wählen Sie im Dialogfeld „Netzwerk" (Register „Konfiguration") den Eintrag „TCP/IP", und klicken Sie auf „Eigenschaften".
2. Klicken Sie auf die Registerkarte „IP-Adresse".
3. Klicken Sie auf „IP-Adresse automatisch beziehen".
4. Klicken Sie auf die Registerkarte „DNS-Konfiguration". Wählen Sie „DNS deaktivieren".
5. Klicken Sie auf die Registerkarte „Gateway". Markieren Sie alle eventuell vorhandenen Gateways, und klicken Sie auf die Schaltfläche „Entfernen", bis kein Gateway mehr in der Liste vorhanden ist.
6. Klicken Sie auf „OK", um die Änderungen zu übernehmen und das Dialogfeld „TCP/IP-Eigenschaften" zu schließen.
7. Klicken Sie auf „OK", um das Dialogfeld „Netzwerk" zu schließen.
8. Starten Sie Ihren Computer neu, wenn Sie dazu aufgefordert werden. Legen Sie Ihre Windows-CD ein, falls Sie dazu aufgefordert werden.

TCP/IP-Einstellungen überprüfen

1. Klicken Sie auf „Start", und wählen Sie den Befehl „Ausführen".
2. Geben Sie im Fenster „Ausführen" den Befehl „winipcfg" ein, und klicken Sie auf „OK", um das Fenster „IP-Konfiguration" zu öffnen.
3. Wählen Sie Ihre Netzwerkkarte aus. Daraufhin werden Informationen zur IP-Adresse, der Subnet-Maske und dem Standard-Gateway Ihres Computers angezeigt.

Eine ausführlichere Anleitung finden Sie auf der beiliegenden CD-ROM.

Computer mit Windows NT/2000/XP einrichten

TCP/IP einrichten

1. Unter **Windows NT und 2000** klicken Sie in der Task-Leiste auf „Start" – „Einstellungen" – „System steuerung" – „Netzwerk und DFÜ-Verbindungen" und dann mit der rechten Maustaste auf „LAN-Verbindung" oder die einzurichtende Verbindung. Wählen Sie die Option „Eigenschaften" aus dem erscheinenden Kontextmenü.
   Unter **Windows XP** wählen Sie „Start" – „Systemsteuerung" – „Netzwerk" – „Internetverbindungen" und anschließend „Netzwerkverbindungen". Klicken Sie mit der rechten Maustaste auf die Verbindung, die Sie einrichten möchten, und wählen Sie „Eigenschaften".
2. Wählen Sie „Internetprotokoll (TCP/IP)" (unter Windows XP im Register „Allgemein"), und klicken Sie auf „Eigenschaften".
3. Daraufhin erscheint das Fenster „Eigenschaften von Internetprotokoll (TCP/IP)". Klicken Sie auf „IP-Adresse automatisch beziehen".
4. Klicken Sie auf „DNS-Serveradresse automatisch beziehen".
5. Klicken Sie auf „Erweitert", öffnen Sie das Register „IP-Einstellungen", und entfernen Sie alle evtl. installierten Gateways. Bestätigen Sie anschließend mit „OK".
6. Klicken Sie auf „OK", um die Änderungen zu speichern und das Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)" zu schließen.
7. Achten Sie darauf, dass im Dialogfeld „Eigenschaften von LAN-Verbindung" ausschließlich die Komponente „Internetprotokoll (TCP/IP)" aktiviert ist, und klicken Sie auf „OK", um das Fenster zu schließen.
8. Starten Sie Ihren Computer neu, wenn Sie dazu aufgefordert werden.

TCP/IP-Einstellungen überprüfen

1. Klicken Sie in der Task-Leiste auf „Start" – „Programme" – „Zubehör" und wählen Sie „Eingabeaufforderung".
2. Geben Sie im Fenster „Eingabeaufforderung" den Befehl „ipconfig" ein, und drücken Sie die Eingabetaste. Daraufhin werden Informationen zur IP-Adresse,der Subnet-Maske und dem Standard-Gateway Ihres Computers angezeigt.

Eine ausführlichere Anleitung finden Sie auf der beiliegenden CD-ROM.

Erstkonfiguration des Teledat Routers 800

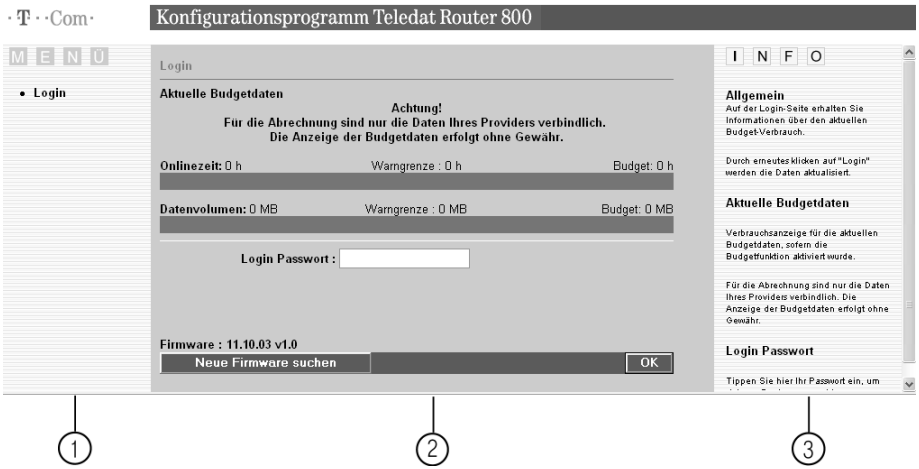
Ihr Teledat Router ist bereits so vorkonfiguriert, dass er im Regelfall ohne umfangreiche Feinkonfiguration lauffähig ist. Daher empfehlen wir, die Erstinstallation mit Hilfe des Assistenten vorzunehmen. Der Assistent ist in den Web-Konfigurator integriert und führt Sie durch wenige Bereiche, die für den Betrieb unabdingbar sind (Schnellkonfiguration). Sie können danach jederzeit eine Feinkonfiguration durchführen.

Der Web-Konfigurator

Der Web-Konfigurator basiert auf HTML. Sie rufen den Web-Konfigurator über einen Internet-Browser auf, indem Sie die IP-Adresse des Routers eingeben. Im Beispiel ist der Internet Explorer® der Microsoft Corporation dargestellt. Sie können ebenso den Netscape Navigator®, Opera® oder andere verwenden.

Öffnen Sie Ihren Internet-Browser. Rufen Sie den Web-Konfigurator auf, indem Sie die IP-Adresse Ihres Teledat Routers eingeben. Diese lautet bei Auslieferung: **192.168.1.1**.
Bestätigen Sie Ihre Eingabe mit **Enter**.

Zunächst wird der grundlegende Bildschirmaufbau erklärt.

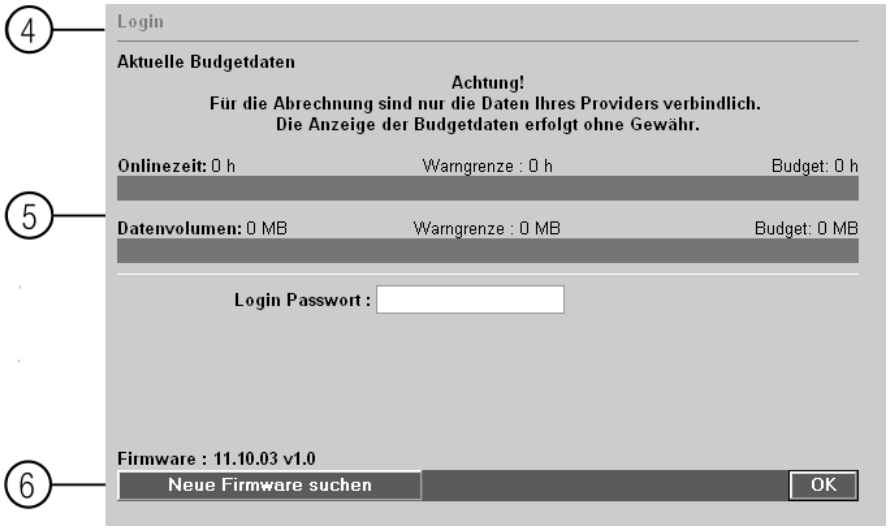

T · · Com ·
Konfigurationsprogramm Teledat Router 800
M E N Ü
Login
I N F O
Login
Aktuelle Budgetdaten
Achtung!
Für die Abrechnung sind nur die Daten Ihres Providers verbindlich.
Die Anzeige der Budgetdaten erfolgt ohne Gewähr.
Onlinezeit: 0 h
Warngrenze : 0 h
Budget: 0 h
Datenvolumen: 0 MB
Warngrenze : 0 MB
Budget: 0 MB
Login Passwort :
Firmware : 11.10.03 v1.0
Neue Firmware suchen
OK
Allgemein
Auf der Login-Seite erhalten Sie Informationen über den aktuellen Budget-Verbrauch.
Durch erneutes klicken auf "Login" werden die Daten aktualisiert.
Aktuelle Budgetdaten
Verbrauchsanzeige für die aktuellen Budgetdaten, sofern die Budgetfunktion aktiviert wurde.
Für die Abrechnung sind nur die Daten Ihres Providers verbindlich. Die Anzeige der Budgetdaten erfolgt ohne Gewähr.
Login Passwort
Tippen Sie hier Ihr Passwort ein, um
1
2
3

Der Konfigurator ist im wesentlichen in drei Bereiche untergliedert. Links befindet sich die **Menüleiste (1)** und rechts der Bereich **Info (3)**. Den Hauptbereich in der Mitte des Fensters nimmt die aktuelle **Konfigurationsseite** (2) ein.

In der **Menüleiste** sind die einzelnen Konfigurationsseiten aufgeführt. Mit Klick auf einen Eintrag, zum Beispiel **Basiskonfiguration**, wird dessen Untermenü angezeigt. Durch Klick auf einen Menüeintrag, zum Beispiel **Passwort** öffnet sich die zugehörige Konfigurationsseite. Über die Menüleiste können Sie jederzeit von einer Konfigurationsseite zu einer anderen wechseln.

Der Bereich **INFO** zeigt Ihnen zu jeder einzelnen Konfigurationsseite Hinweise und Erläuterungen, die Sie bei der Konfiguration unterstützen sollen.

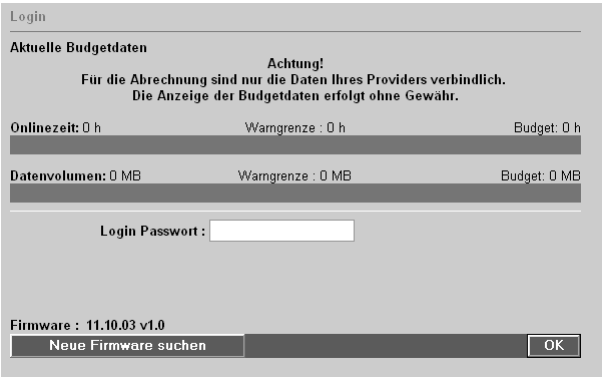
Die einzelnen **Konfigurationsseiten** sind in Kopfbereich (4), Fußbereich (6) und Hauptteil (5) gegliedert.



Im **Kopfbereich** befindet sich die **Bezeichnung** des Menüs. Diese stimmt mit der Bezeichnung in der Menüleiste überein. Speziell bei mehrfach verschachtelten Menüs soll Ihnen so die Orientierung erleichtert werden.

Im **Fußbereich** sind die **Befehlsschaltflächen** platziert. In den meisten Menüs finden Sie die Tasten **OK** für Eingaben speichern und **Abbrechen** für Eingabe rückgängig machen. Zusätzliche Schaltflächen sind im jeweiligen Infobereich erklärt.

Im **Hauptteil** der einzelnen Konfigurationsseiten nehmen Sie Ihre Einstellungen vor oder können zum Beipiel im Bereich Status wichtige Informationen abrufen.



Beim **erstmaligen Aufruf** Ihres Web-Konfigurators werden Sie aufgefordert, das Passwort für den Teledat Router anzugeben.

Im Auslieferungszustand ist das Passwort **1234** eingestellt. Tragen Sie dieses unter **Login Passwort** ein.

Bestätigen Sie Ihre Eingabe durch Klick auf **OK**.

Microsoft Internet Explorer
Sie sollten das Passwort nicht auf der Werkseinstellung belassen.
Bitte ändern Sie das Passwort!
OK

Nach Eingabe des Passwortes **1234**, werden Sie aufgefordert, ein neues Passwort zu vergeben.

Klicken Sie auf **OK**.

Geben Sie zunächst unter **Altes Passwort** das bestehende ein (bei Erstinbetriebnahme ist das Passwort **1234** vergeben).

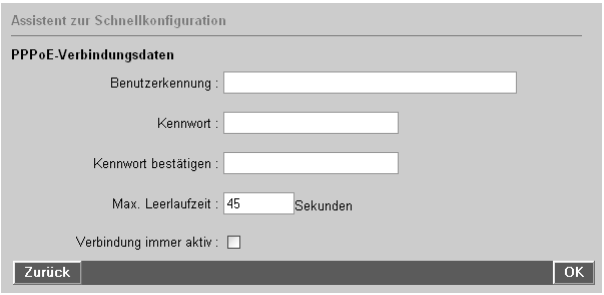
Klicken Sie anschließend in das Eingabefeld **Neues Passwort** und geben Sie ein neues Passwort ein. Im Eingabefeld **Passwort bestätigen** wiederholen Sie die Eingabe Ihres neuen Passwortes. Aktivieren Sie Ihre Änderung, indem Sie auf **OK** klicken.

Sie können jetzt den Assistenten starten, der Sie durch die wichtigsten Menüs zur Routerkonfiguration führt.

Klicken Sie hier auf **OK**, um den Assistenten zu starten.

Erstkonfiguration mit dem Assistenten

Mit Hilfe des Assistenten können Sie die wichtigsten Einstellungen für die Inbetriebnahme Ihres Teledat Routers vornehmen.



Geben Sie hier die Daten für Ihren Internetzugang an, die Sie von T-Online oder Ihrem **ISP** (Internet Service Provider) erhalten haben.

Tragen Sie **Benutzerkennung** und **Kennwort** ein. Wiederholen Sie die Eingabe des Kennworts bei **Kennwort bestätigen**.

Tipp

Für einen T-Online-Zugang mit der Anschlusskennung 000123456789, T-Online-Nummer 091131410099 und Mitbenutzernummer 0001 ergibt sich beispielsweise folgende Benutzerkennung: 000123456789091131410099#0001@t-online.de.

Tragen Sie die **Max. Leerlaufzeit** ein. Diese Zeit gibt an, wie lange eine Verbindung bestehen bleibt, wenn keine Daten übertragen werden. Im Beispiel heißt das, nach 45 Sekunden ohne Datentransfer wird die bestehende Verbindung beendet.

Aktivieren Sie die Option **Verbindung immer aktiv**, baut der Router die Verbindung nicht ab, sondern bleibt immer online.

!

Wir empfehlen, diese Option nur zu aktivieren, wenn Sie über eine Flatrate oder über einen Datenvolumen-Tarif verfügen. Ansonsten können hierbei sehr hohe Kosten anfallen.

Bestätigen Sie Ihre Auswahl mit **OK**.

Im folgenden Fenster werden Ihre Einstellungen zusammenfassend dargestellt. Ist alles korrekt, schließen Sie die Konfiguration durch Klick auf **OK** ab.

Damit ist die Konfiguration Ihres Internetzugangs abgeschlossen, den Sie jetzt direkt testen können.

Optional können Sie aber auch schon die Budgetinformationen erfassen. Details hierzu finden Sie im Referenzteil dieses Handbuches ab Seite 27.

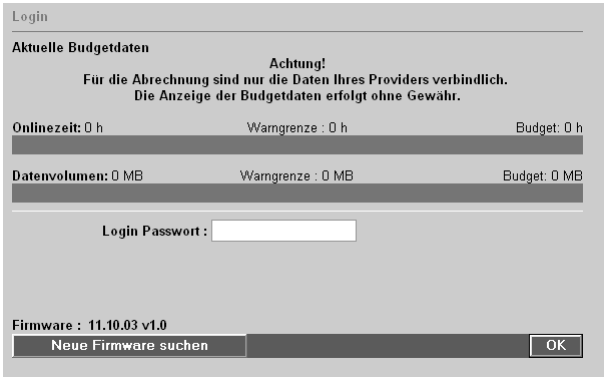
Teledat Router 800 konfigurieren

Dieses Kapitel beschreibt die Konfigurationseinstellungen des Teledat Routers. Diese umfassen sowohl die Basiskonfiguration als auch erweiterte Einstellungen, zum Beispiel die Konfiguration der Firewall oder die Einrichtung entfernter Nutzer.

!

Einige dieser erweiterten Einstellungen sollten Sie nur vornehmen, wenn Sie sich sicher sind, was sie bewirken. Zum Beispiel können infolge einiger Einstellungen Schutzfunktionen Ihres Teledat Routers ausgeschaltet werden.

Login



Im oberen Bereich der Konfigurationsseite können Sie **Aktuelle Budgetdaten** ablesen.

Haben Sie die Konfiguration Ihrer **Budgetkontrolle** (siehe Seite 28) bereits vorgenommen, werden die aktuellen Verbrauchswerte, Warngrenzen und Budgets für Onlinezeit und Datentransfervolumen angezeigt.

Beim erstmaligen Aufruf des Konfigurators sind die Werte mit Null (0) belegt.

Im Fußbereich wird die aktuell installierte Version der Firmware angezeigt. Haben Sie Ihren Internetzugang bereits konfiguriert, gelangen Sie durch Klick auf **Neue Firmware suchen** zur Internetseite der T-Com - www.telekom.de/teledatrouter800. Hier stehen für Sie gegebenenfalls aktuellere Versionen der Firmware zum Download zur Verfügung.

Tipp

Auf unserer Internetsite können Sie sich zur Wahrung der sowohl zum Zeitpunkt des Kaufs bereits aktivierten als auch der durch Sie selbst veranlassten Sicherheitseinstellungen regelmäßig über aktuelle Hinweise zu Ihrem Produkt informieren und ggf. neue Software-Versionen herunterladen.

Geben Sie nun im mittleren Bereich unter **Login Passwort** das Passwort für Ihren Teledat Router ein. Bei Auslieferung ist das Passwort **1234** eingestellt. Bei der ersten Inbetriebnahme Ihres Teledat Routers tragen Sie dieses bitte ein. Bestätigen die Eingabe durch Klick auf **OK**.

Home

Nach dem Login oder durch Klick auf **Home** in der Menüleiste Ihres Teledat Routers öffnet sich nebenstehendes Statusfenster.

Hier erhalten Sie einen Überblick über Ihre Internetaktivitäten.

Im Bereich **Status** können Sie erkennen, ob die **Budgetkontrolle** aktiviert ist. Zusätzlich wird angezeigt, seit wann der **Router in Betrieb** ist (ohne Neustart).

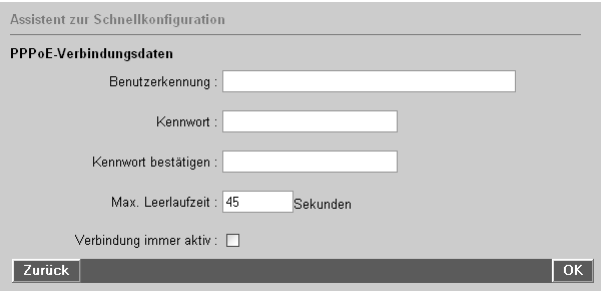
Der Abschnitt **Aktuelle Budgetdaten** informiert Sie über das übertragene **Datenvolumen** und Ihre **Onlinezeit** im aktuellen Abrechnungszeitraum. Zusätzlich sind die **Budgets** und **Warngrenzen** sowie der Beginn des **Abrechnungszeitraumes** angegeben.

!

Für die Abrechnung sind nur die Daten Ihres Providers verbindlich. Die Anzeige der Budgetdaten erfolgt ohne Gewähr.

Im Bereich **WAN-Status** wird die aktuelle **IP-Adresse** Ihres Teledat Routers im Intranet angezeigt. Der **Modus** gibt an, welche Art von Breitbandzugriff aktiv ist: PPPoE, PPTP oder Standleitung. Die **Zeit** gibt die Dauer der aktuellen Verbindung an. Über **Auflegen** können Sie die Verbindung beenden. Über **Anwählen** können Sie eine Verbindung manuell aufbauen.

Assistent



Wählen Sie in der Menüleiste Ihres Teledat Routers den Eintrag **Assistent**.

Jetzt wird der Assistent zur Schnellkonfiguration gestartet.

Mit dessen Hilfe könnn Sie die wichtigsten Einstellungen zur Inbetriebnahme Ihres Teledat Routers vornehmen.

Eine genaue Beschreibung der einzelnen Schritte des Assistenten finden Sie im Abschnitt **Erstkonfiguration des Teledat Routers** ab Seite 15 in diesem Handbuch.

Basiskonfiguration

Die Konfigurationsseiten für die Basiskonfiguration umfassen die Grundeinstellungen Ihres Teledat Routers.

Passwort

Hier richten Sie das Login-Passwort Ihres Teledat Routers ein.

Wir empfehlen Ihnen, ein Passwort einzurichten, dass sich von dem des Lieferzustandes (1234) unterscheidet.

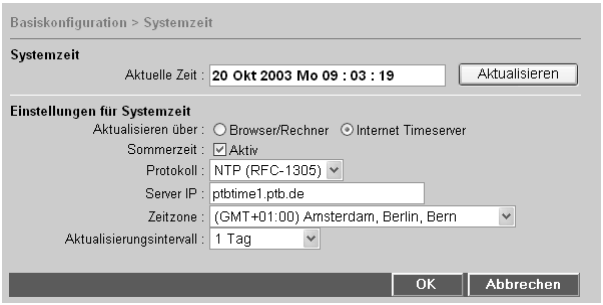
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Basiskonfiguration** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Passwort**.

Geben Sie unter **Altes Passwort** das bestehende ein (werksseitig ist das Passwort **1234** vergeben). Klicken Sie anschließend in das Eingabefeld **Neues Passwort** und geben Sie das neue Passwort ein.

Im Eingabefeld **Passwort bestätigen** wiederholen Sie die Eingabe Ihres neuen Passwortes.

Aktivieren Sie Ihre Änderung, indem Sie auf **OK** klicken.

Systemzeit



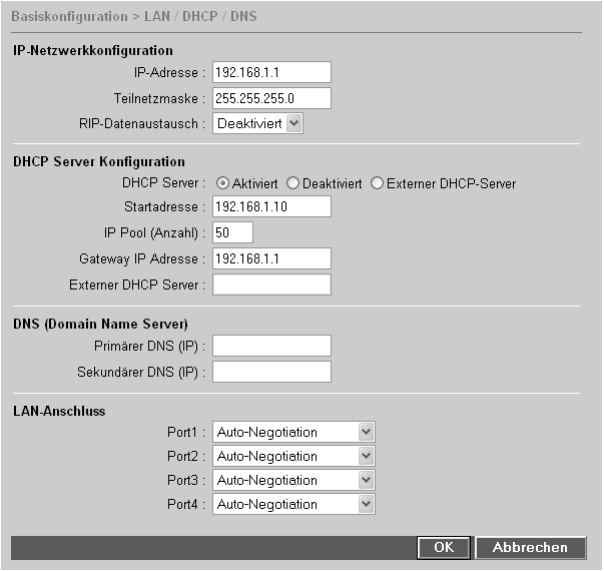
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Basiskonfiguration** und wählen Sie aus dem Untermenü den Eintrag **Systemzeit**.

Unter **Systemzeit** wird die **Aktuelle Zeit** Ihres Teledat Routers angezeigt.

Klicken Sie auf **Aktualisieren**, um die Zeit neu zu übernehmen. Im Bereich **Einstellungen für Systemzeit** geben Sie bitte an, ob die Zeiteinstellungen vom **Browser/Rechner** oder von einem **Internet Timeserver** übernommen werden sollen.

Haben Sie **Internet Timeserver** gewählt, prüfen Sie bitte die weiteren Einstellungen in diesem Fenster. Im Zeitraum der europäischen Sommerzeit aktivieren Sie bitte **Sommerzeit**. Es erfolgt keine automatische Umstellung zwischen Sommer- und Winterzeit. Geben Sie die **Server IP** des Timeservers an. Im Lieferzustand ist die Option **Internet Timeserver** aktiviert und der Server der Physikalisch-Technischen Bundesanstalt in Braunschweig (ptbtime1.ptb.de) voreingestellt. Wir empfehlen Ihnen, diese Einstellungen beizubehalten. Prüfen Sie nun die korrekte Angabe Ihrer **Zeitzone** und geben Sie den **Aktualisierungsintervall** an. Nach Ablauf der hier eingestellten Zeit wird die Systemzeit des Routers mit der des Timeservers abgeglichen. Diese Synchronisation erfolgt nur dann, wenn der Router online ist.

Möchten Sie zum Beispiel die Funktionen Verbindungstimer, SysLog oder Budgetkontrolle anwenden, ist eine korrekte Einstellung der Systemzeit erforderlich.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Basiskonfiguration** und wählen Sie aus dem Untermenü den Eintrag **LAN/DHCP/DNS** aus.

Hier nehmen Sie die Einstellungen für LAN, DHCP und DNS vor.

Konfigurieren Sie unter **IP-Netzwerkkonfiguration** Ihren Router für das LAN.

Tragen Sie die **IP-Adresse** des Routers im lokalen Netzwerk ein. Diese Adresse geben Sie bei den angeschlossenen Rechnern als Router-Adresse an.

Tragen Sie ebenfalls die **Teilnetzmaske** des Routers ein. Ab Werk sind die IP-Adresse 192.168.1.1 und die Teilnetzmaske 255.255.255.0 voreingestellt. Wenn noch kein TCP/IP-Netz vorhanden ist, können Sie die Voreinstellungen beibehalten. Mittels DHCP erhalten dann alle Rechner im Netz eine zum Router passende Konfiguration.

Aktivieren Sie die Option **RIP Datenaustausch**, wenn das RIP-Protokoll genutzt werden soll.

Tipp

Haben Sie Rechnern im Netzwerk feste IP-Adressen vergeben, beachten Sie bitte folgendes: Weisen Sie dem Router eine andere Adresse und/oder eine andere Teilnetzmaske zu, müssen Sie die TCP/IP Einstellungen der Rechner entsprechend anpassen, damit diese den Router mit den neuen Einstellungen weiterhin erreichen können. Jeder Rechner benötigt die neue IP-Adresse des Routers und muss sich im selben Teilnetz befinden wie die Router!

Um die Verwaltung der IP-Adressen zu vereinfachen, können Sie Ihren Teledat Router als DHCP-Server einsetzen. In diesem Fall konfigurieren Sie Ihre Rechner als DHCP-Clients (siehe Seite 9). Jedem dieser Rechner wird automatisch eine IP-Adresse vom Router zugewiesen, die in der Regel bis zum nächsten Neustart beibehalten wird. Gleichzeitig übergibt der Router die Angaben zu Teilnetzmaske und Gateway-Adresse (im Allgemeinen die des Routers) an die Rechner. Ändern Sie die IP-Adresse des Routers, passt dieser die Startadresse für den DHCP-Server automatisch entsprechend an.

Bei **DHCP-Server** können Sie zwischen folgenden drei Alternativen wählen:

1. Möchten Sie den Router als DHCP-Server einsetzen, wählen Sie die Option **Aktiviert** für **DHCP Server**. Die **Startadresse** gibt die erste vom DHCP-Server zu vergebende IP-Adresse für DHCP-Clients an. Die Adressen werden jeweils im letzten Segment variiert. Die Startadresse muss im Adressbereich des Routers liegen (wird durch die **IP-Adresse** und **Teilnetzmaske** vorgegeben).

   Die Angabe bei **IP Pool** bestimmt die maximale Anzahl der zu vergebenden Adressen. Im gezeigten Beispiel bedeutet das: Die erste zu vergebende IP Adresse ist die 192.168.1.10 und es werden nach Bedarf Adressen bis 192.168.1.59 vergeben.

   Die **Gateway IP Adresse** bestimmt, welche IP Adresse DHCP-Clients vom Teledat Router zur Einwahl ins Internet erhalten. In der Regel soll der Internetzugang über den Router selbst erfolgen, deshalb ist dessen IP voreingestellt.

2. Wenn Sie die DHCP-Server-Funktion nicht nutzen möchten, zum Beispiel weil Sie nur mit statischen Adressen arbeiten wollen, wählen Sie die Option **Deaktiviert**.

3. Ist bereits ein DHCP-Server im Netz vorhanden, so kann Ihr Teledat Router die DHCP-Anfragen an diesen Server weiterleiten. Aktivieren Sie in diesem Fall **Externer DHCP-Server** und tragen dessen IP-Adresse im zugehörigen Feld ein.

Tipp

Für Rechner mit besonderen Aufgaben in Ihrem LAN, zum Beispiel Rechner die über eine Portumleitung aus dem Internet erreichbar sein sollen (siehe Portumleitung auf Seite 64), empfehlen wir die Vergabe von festen IP-Adressen. Beachten Sie, dass sich diese Adressen ausserhalb des definierten IP-Pools befinden müssen.

Wenn Sie Domain Name Server angeben möchten, die zum Beispiel von Ihrem ISP angeboten werden, tragen Sie deren IP-Adressen im Bereich **DNS (Domain Name Server)** unter **Primärer DNS (IP)** beziehungsweise **Sekundärer DNS (IP)** ein.

Im Abschnitt **LAN-Anschluss** können Sie die Übertragungsgeschwindigkeit für die einzelnen LAN-Ports festlegen. Wählen Sie zum Beispiel **Auto-Negotiation** erfolgt eine automatische Geschwindigkeitsanpassung. Alternativ können Sie die Geschwindigkeit mit 100 oder 10 MBits pro Sekunde Voll- beziehungsweise Halb-Duplex festlegen.

Tipp

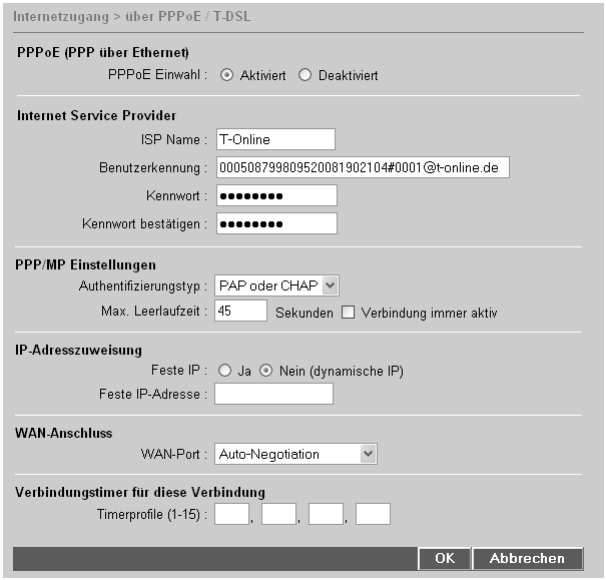
Haben Sie bei einer LAN-Verbindung beispielsweise Schwierigkeiten bei der Übertragungsgeschwindigkeit von 100 MBit/s, können Sie diese für den betreffenden Port mit 10 MBit/s festlegen, um eine sicherere Datenübertragung zu erreichen.

Bestätigen Sie Ihre Änderungen mit **OK**. Ihr Router wird anschließend neu gestartet.

Internetzugang

PPPoE / T-DSL

Auf der folgenden Seite können Sie Ihren Breitbandzugang über PPPoE/ T-DSL konfigurieren.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Internetzugang** und wählen Sie aus dem Untermenü den Eintrag **PPPoE/T-DSL**.

Aktivieren Sie Ihren Breitbandzugang, indem Sie für **PPPoE Einwahl** die Auswahl **Aktiviert** markieren.

Tragen Sie im Bereich **Internet Service Provider** den Namen Ihres ISP (frei wählbar, zum Beispiel T-Online) im Feld **ISP Name** ein.

Geben Sie in den folgenden Feldern Ihre **Benutzerkennung** und Ihr **Kennwort** ein. Wiederholen Sie die Eingabe Ihres Kennwortes unter **Kennwort bestätigen**. Entnehmen Sie diese Angaben den Unterlagen, die Sie von Ihrem ISP erhalten haben.

Tipp

Für einen T-Online-Zugang mit der Anschlusskennung 000123456789, T-Online-Nummer 091131410099 und Mitbenutzernummer 0001 ergibt sich beispielsweise folgende Benutzerkennung: 000123456789091131410099#0001@t-online.de.

Die Daten zur Authentifizierung wurden Ihnen von Ihrem ISP vertraulich übergeben. Bewahren Sie diese Daten unzugänglich für Unbefugte auf.

Nehmen Sie ebenfalls die **PPP/MP Einstellungen** vor. Die Authentifizierung kann über PAP oder CHAP erfolgen. In der Regel können Sie daher unter **Authentifizierungstyp** den Eintrag **PAP oder CHAP** stehen lassen. Nur in Ausnahmefällen ist das Umstellen auf **Nur PAP** nötig.

Tragen Sie ebenfalls die **Max. Leerlaufzeit** Ihres Teledat Routers ein. Diese Zeit gibt an, wie lange eine Verbindung bestehen bleibt, wenn keine Daten übertragen werden. Im Beispiel heißt das, nach 45 Sekunden ohne Datentransfer wird die bestehende Verbindung beendet. Aktivieren Sie die Option **Verbindung immer aktiv**, baut der Router die PPPoE-Verbindung nicht ab, sondern bleibt immer online.

!

Wir empfehlen, diese Option nur zu aktivieren, wenn Sie über eine Flatrate oder über einen Datenvolumen-Tarif verfügen. Ansonsten können hierbei sehr hohe Kosten anfallen.

Geben Sie an, wie die IP-Adresse zugewiesen werden soll, über die der Router aus dem Internet erreichbar sein soll. Im Regelfall wird keine feste IP vergeben, sondern sie wird bei jeder Anwahl vom ISP neu (dynamisch) zugewiesen. Aktivieren Sie daher bei **IP-Adresszuweisung** für die Option **Feste IP** das **Nein (dynamische IP)** und nehmen unter **Feste IP-Adresse** keinen Eintrag vor. Erhalten Sie von Ihrem ISP andere Vorgaben, tragen Sie diese entsprechend ein.

Im Bereich **WAN-Anschluss** können Sie die Übertragungsgeschwindigkeit für den **WAN-Port** festlegen. Wählen Sie zum Beispiel **Auto-Negotiation** erfolgt eine automatische Geschwindigkeitsanpassung. Alternativ können Sie die Geschwindigkeit mit 100 oder 10 MBits pro Sekunde Voll- beziehungsweise Halb-Duplex festlegen.

Tipp

Haben Sie bei einer LAN-Verbindung beispielsweise Schwierigkeiten bei der Übertragungsgeschwindigkeit von 100 MBit/s, können Sie diese für den betreffenden Port mit 10 MBit/s festlegen, um eine sicherere Datenübertragung zu erreichen.

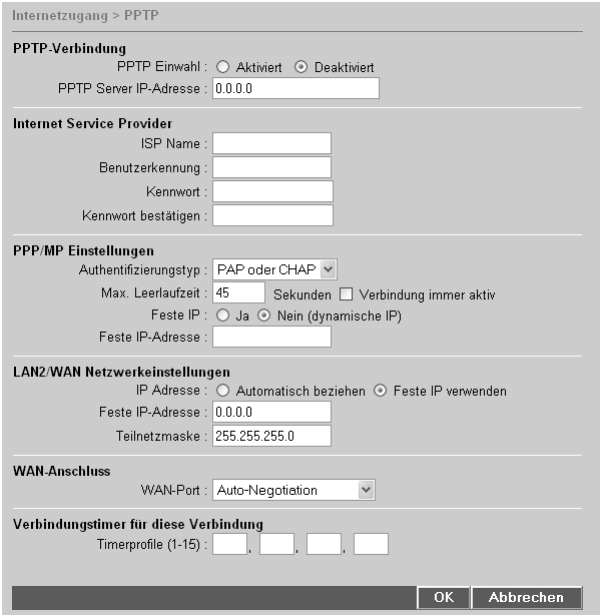
Möchten Sie Timereinstellungen (siehe Seite 56) für diese DSL-Verbindung aktivieren, tragen Sie die zugehörigen Indexwerte (maximal vier) unter **Verbindungstimer für diese Verbindung** ein.

Bestätigen Sie Ihre Eingaben mit **OK**.

Die Konfiguration Ihres Breitband-Zuganges über PPPoE / T-DSL ist nun abgeschlossen. Sie können jetzt im Internet surfen.

PPTP

Auf der folgenden Seite können Sie Ihren Breitbandzugang über PPTP konfigurieren.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Internetzugang** und wählen Sie aus dem Untermenü den Eintrag **PPTP**.

Aktivieren Sie Ihren Breitbandzugang indem Sie für **PPTP Einwahl** die Auswahl **Aktiviert** markieren.

Tragen Sie die IP-Adresse des PPTP-Servers unter **PPTP Server IP-Adresse** ein. Diese können Sie in der Regel der Dokumentation Ihres ISPs oder DSL-Modems entnehmen. Sie wird benötigt, um die Verbindung zwischen Router und DSL-Modem aufzubauen.

Tragen Sie im Bereich **Internet Service Provider** die Angaben zu Ihrem ISP ein. Geben Sie in den folgenden Feldern **ISP-Name** (frei wählbar), Ihre **Benutzerkennung** und Ihr **Kennwort** ein. Wiederholen Sie die Eingabe Ihres Kennwortes unter **Kennwort bestätigen**. Entnehmen Sie diese Angaben den Unterlagen, die Sie von Ihrem ISP erhalten haben. Die Daten zur Authentifizierung wurden Ihnen von Ihrem ISP vertraulich übergeben. Bewahren Sie diese Daten unzugänglich für Unbefugte auf.

Nehmen Sie im Folgenden die **PPP Einstellungen** vor. Die Authentifizierung kann über PAP oder CHAP erfolgen. In der Regel können Sie daher unter **Authentifizierungstyp** den Eintrag **PAP oder CHAP** stehen lassen. Nur in Ausnahmefällen ist das Umstellen auf **Nur PAP** nötig.

Tragen Sie ebenfalls die **Max. Leerlaufzeit** Ihres Teledat Routers ein. Diese Zeit gibt an, wie lange eine Verbindung bestehen bleibt, wenn keine Daten übertragen werden. Im Beispiel heißt das, nach 45 Sekunden ohne Datentransfer wird die bestehende Verbindung beendet.

Aktivieren Sie die Option **Verbindung immer aktiv**, baut der Router die PPTP-Verbindung nicht ab, sondern bleibt immer online.

!

Wir empfehlen, diese Option nur zu aktivieren, wenn Sie über eine Flatrate oder über einen Datenvolumen-Tarif verfügen. Ansonsten können hierbei sehr hohe Kosten anfallen.

Geben Sie an, wie die IP-Adresse zugewiesen werden soll, über die der Router aus dem Internet erreichbar sein soll. Im Regelfall wird keine feste IP vergeben, sondern sie wird bei jeder Anwahl vom ISP neu (dynamisch) zugewiesen. Aktivieren Sie daher bei **IP-Adresszuweisung** für die Option **Feste IP** das **Nein (dynamische IP)** und nehmen unter **Feste IP-Adresse** keinen Eintrag vor. Erhalten Sie von Ihrem ISP andere Vorgaben, tragen Sie diese entsprechend ein.

Die **LAN2/WAN Netzwerkeinstellungen** beziehen sich auf die Verbindung zwischen dem DSL-Modem und dem Router. Aktivieren Sie die PPTP-Einwahl, wird automatisch die Option **Feste IP verwenden** aktiviert und Vorgabewerte für **IP-Adresse** und **Teilnetzmaske** eingetragen. Wie empfehlen diese Einstellungen beizubehalten, es sei denn Sie erhalten von Ihrem ISP abweichende Vorgaben.

Im Bereich **WAN-Anschluss** können Sie die Übertragungsgeschwindigkeit für den **WAN-Port** festlegen. Wählen Sie zum Beispiel **Auto-Negotiation** erfolgt eine automatische Geschwindigkeitsanpassung. Alternativ können Sie die Geschwindigkeit mit 100 oder 10 MBits pro Sekunde Voll- beziehungsweise Halb-Duplex festlegen.

Tipp

Haben Sie bei einer LAN-Verbindung beispielsweise Schwierigkeiten bei der Übertragungsgeschwindigkeit von 100 MBit/s, können Sie diese für den betreffenden Port mit 10 MBit/s festlegen, um eine sicherere Datenübertragung zu erreichen.

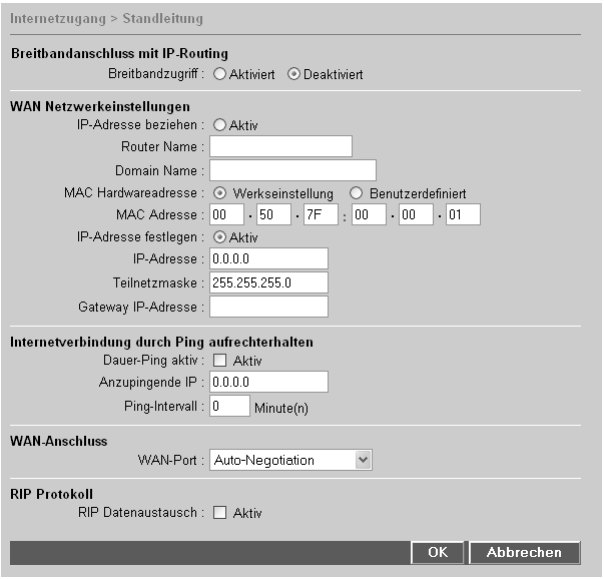
Möchten Sie Timereinstellungen (siehe Seite 56) für diese DSL-Verbindung aktivieren, tragen Sie die zugehörigen Indexwerte (maximal vier) unter **Verbindungstimer für diese Verbindung** ein.

Bestätigen Sie Ihre Eingaben mit **OK**.

Die Konfiguration Ihres Breitband-Zuganges über PPTP ist nun abgeschlossen. Sie können jetzt im Internet surfen.

Standleitung

Auf der folgende Seite können Sie Ihren Breitbandzugang über eine Standleitung konfigurieren.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Internetzugang** und wählen Sie aus dem Untermenü den Eintrag **Standleitung**.

Aktivieren Sie Ihren Breitbandzugang indem Sie für **Breitbandzugriff** die Auswahl **Aktiviert** markieren.

Geben Sie unter **WAN Netzwerkeinstellungen** die Daten für Ihre Standleitung ein. Die Option **IP-Adresse automatisch beziehen** wird nicht aktiviert, da im Regelfall die IP-Adresse im Teledat Router festgelegt wird.

Tipp

Sollte in Ihrem Fall dennoch die IP-Adresse automatisch bezogen werden, informieren Sie sich bei Ihrem ISP, ob die Angaben zu **Router Name** und **Domain Name** benötigt werden. Wenn ja, nehmen Sie bitte die Eintragungen vor.

Wählen Sie bei **MAC-Hardwareadresse** die **Werkseinstellung** oder **Benutzerdefiniert**. Im Regelfall aktivieren Sie die Option **IP-Adresse festlegen**. Tragen Sie unter **IP-Adresse** die öffentlich zugängliche Internet-IP-Adresse Ihres Teledat Routers ein. Diese Adresse muss sich in dem Adressraum befinden, der Ihnen von Ihrem ISP zugeteilt wurde. Die Daten zu **Teilnetzmaske** und **Gateway IP-Adresse** erhalten Sie ebenfalls von Ihrem ISP. Als Gateway tragen Sie die IP-Adresse Ihres Übergaberouters ein.

Möchten Sie Ihre Internetverbindung dauerhaft aufrechterhalten, aktivieren Sie die Option **Dauer-Ping aktiv**. Tragen Sie dann ebenfalls die **Anzupingende IP** und das **Ping-Intervall** ein.

Im Bereich **WAN-Anschluss** können Sie die Übertragungsgeschwindigkeit für den **WAN-Port** festlegen. Wählen Sie zum Beispiel **Auto-Negotiation** erfolgt eine automatische Geschwindigkeitsanpassung. Alternativ können Sie die Geschwindigkeit mit 100 oder 10 MBits pro Sekunde Voll- beziehungsweise Halb-Duplex festlegen.

Tipp

Haben Sie bei einer LAN-Verbindung beispielsweise Schwierigkeiten bei der Übertragungsgeschwindigkeit von 100 MBit/s, können Sie diese für den betreffenden Port mit 10 MBit/s festlegen, um eine sicherere Datenübertragung zu erreichen.

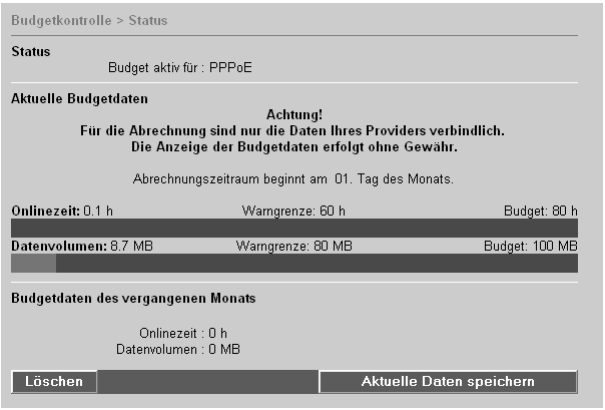
Aktivieren Sie die Option **RIP Datenaustausch**, wenn das RIP-Protokoll genutzt werden soll.

Bestätigen Sie Ihre Eingaben mit **OK**.

Die Konfiguration Ihres Breitband-Zuganges über Standleitung ist nun abgeschlossen. Sie können jetzt im Internet surfen.

Budgetkontrolle

Status



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Budget** und wählen Sie aus dem Untermenü den Eintrag **Status**.

Hier können Sie aktuelle Informationen zum Stand Ihres Onlinekontos entnehmen.

Klicken Sie auf **Löschen**, um den Verbrauch im aktuellen Abrechnungszeitraum auf Null (0) zurückzusetzen.

Ihr Teledat Router sichert die aktuellen Verbrauchswerte für Verbindungszeit und Transfervolumen regelmäßig einmal pro Stunde in seinem internen Speicher.

Tipp

Möchten Sie Ihre Verbrauchswerte zu einem beliebigen anderen Zeitpunkt sichern, zum Beispiel bevor Sie den Router ausschalten, klicken Sie auf **Aktuelle Daten speichern**.

Im Bereich **Status** können Sie erkennen, ob die **Budgetkontrolle** für den PPPoE-Zugang aktiviert ist.

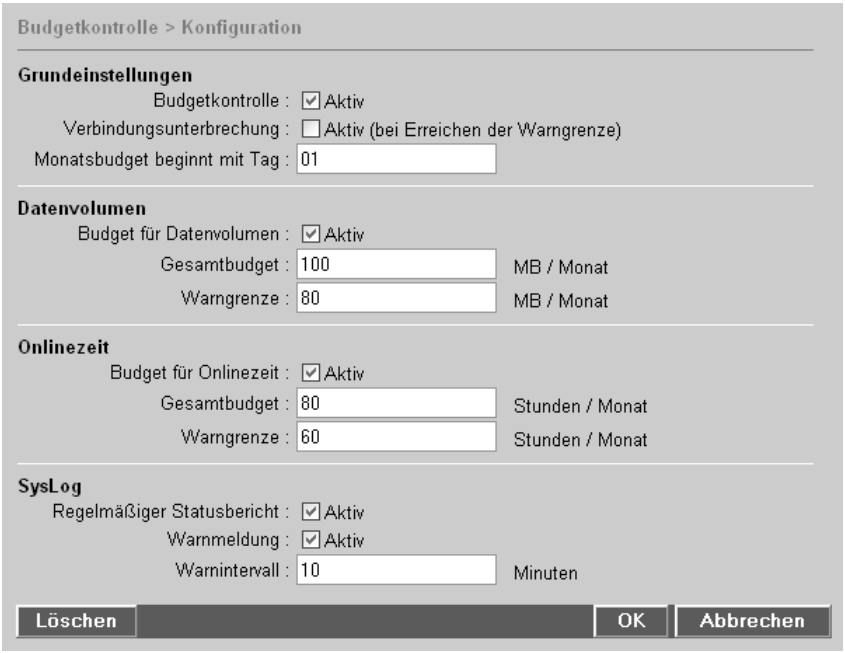
Der Abschnitt **Aktuelle Budgetdaten** informiert Sie über das übertragene **Datenvolumen** und Ihre **Onlinezeit** im aktuellen Abrechnungszeitraum. Zusätzlich sind die **Budgets** und **Warngrenzen** sowie der Beginn des **Abrechnungszeitraumes** angegeben.

Für die Abrechnung sind nur die Daten Ihres Providers verbindlich. Die Anzeige der Budgetdaten erfolgt ohne Gewähr.

Im unteren Teil des Fensters werden die **Budgetdaten des vergangenen Monats** für Onlinezeit und übertragenes Datenvolumen angezeigt.

Konfiguration

Auf der folgenden Konfigurationsseite nehmen Sie die Grundeinstellungen für die Budgetfunktion vor. Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Budget** und wählen Sie aus dem Untermenü den Eintrag **Konfiguration**. Nehmen Sie im Folgenden die Definition Ihres Tarifes vor, den Sie mit Ihrem ISP vereinbart haben.



Um die Funktion zu aktivieren, setzen Sie neben **Budgetkontrolle** einen Haken vor **Aktiv**.

Aktivieren Sie die Option **Verbindungsunterbrechung**, wird die Internetverbindung beendet, sobald eine der eingestellten Warngrenzen erreicht wird.

Im abgebildeten Beispiel wird eine bestehende Verbindung unterbrochen, sobald im aktuellen Abrechnungszeitraum das übertragene Datenvolumen 80 Megabyte überschritten hat oder der Grenzwert für Onlinezeit von 60 Stunden erreicht wurde. Eine Verbindung ist erst wieder möglich, wenn

a) der vorgegebene Stichtag erreicht wird, das heisst wenn ein neuer Abrechnungszeitraum beginnt,
b) Sie manuell die Option **Verbindungsunterbrechung** deaktivieren,
c) Sie die Budgetkontrolle teilweise oder ganz abschalten oder wenn
d) Sie die Warngrenze auf einen höheren Wert einstellen.

Geben Sie unter **Monatsbudget beginnt mit Tag** den Beginn Ihres Abrechnungszeitraumes an. Stichtag eins (**01**) bedeuted, dass das aktuelle Budget vom ersten bis zum letzten Tag des aktuellen Monats berechnet wird.

Aktivieren Sie die Einstellung **Budget für Datenvolumen**, wenn Sie über Ihr Onlinekonto das übertragene Datenvolumen messen möchten. Geben Sie dazu Ihr **Gesamtbudget** und Ihre **Warngrenze** in Megabyte pro Monat an.

Aktivieren Sie die Einstellung **Budget für Onlinezeit**, wenn Sie über Ihr Onlinekonto die Onlinezeit messen möchten. Geben Sie dazu Ihr **Gesamtbudget** und Ihre **Warngrenze** in Stunden pro Monat an.

Die Angaben zu den **Gesamtbudgets** können Sie den Vertragsunterlagen mit Ihrem ISP entnehmen.

Die **Warngrenzen** können Sie individuell festlegen und sowohl für die Onlinezeit als auch für das Datentransfervolumen angeben. Das Erreichen eines Grenzwertes kann folgende Aktionen auslösen:

a) Verbindungsunterbrechung: Beenden der Internetverbindung
b) Warnmeldung über SysLog: Protokollierung der Überschreitung der Grenzwerte.

Die Angabe von Warngrenzen ermöglicht Ihnen somit eine automatische Überwachung der Auslastung Ihres Onlinekontos.

Ihr Teledat Router bietet Ihnen die Möglichkeit, Budgetinformationen zu protokollieren. Die Einstellungen hierfür können Sie im Bereich **SysLog** festlegen.

Möchten Sie in regelmäßigen Abständen Ihren Kontostand protokollieren, aktivieren Sie die Option **Regelmäßiger Statusbericht**.

Setzen Sie einen Haken bei **Warnmeldung**, wird über SysLog eine Meldung erzeugt, die Sie darauf hinweist, dass eine Ihrer definierten Warngrenzen erreicht wurde.

Tragen Sie im Feld **Warnintervall** die Zeitspanne für die Wiederholung der Warnmeldungen in Minuten ein.

Speichern Sie Ihre Eingaben mit **OK**. Klicken Sie auf **Löschen**, werden alle Eintragungen zur Budgetkontrolle gelöscht.

Tipp

Prüfen Sie unter **Verwaltung/SysLog**, ob die Protokollfunktion für die Budgetkontrolle aktiviert ist. Nur dann können Statusmeldungen beziehungsweise Warnmeldungen protokolliert werden. Ausführliche Angaben zur Funktion SysLog finden Sie ab Seite 58 in diesem Handbuch.

Die Warngrenzen im Beispiel wurden so festgelegt, dass sie etwa 80 Prozent des jeweiligen Gesamtbudgets entsprechen. Zusätzlich wurde die Option **Warnmeldung** unter **SysLog** aktiviert. Wird einer der beiden Warngrenzen erreicht, wird im Protokoll der Budgetkontrolle eine entsprechende Meldung erzeugt. Sie wissen jetzt, dass noch etwa 20 Prozent Ihres Onlinebudgets für die restliche Laufzeit des aktuellen Abrechnungszeitraumes zur Verfügung stehen.

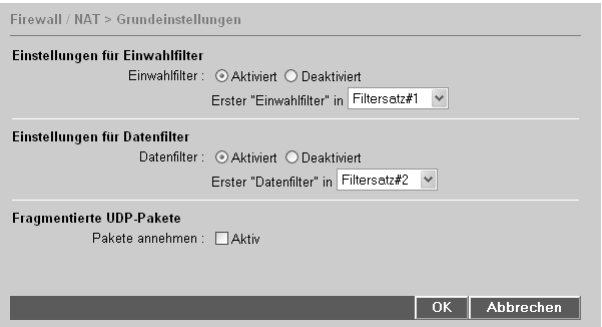
Alternativ dazu können Sie die Warngrenzen auch so festlegen, dass sie mit den Gesamtbudgets übereinstimmen. Aktivieren Sie dann zum Beispiel die **Verbindungsunterbrechung** bei Erreichung der Warngrenze. Diese Einstellungen bewirken, dass nach Erreichen einer Warngrenze die Internetverbindung abgebrochen wird.

Firewall / NAT

Die Firewall blockiert ungerechtfertigte Zugriffe, sowohl aus dem Internet in das interne Netzwerk, als auch vom internen Netzwerk in das Internet.

Die Konfiguration der Firewall sollten Sie nur vornehmen, wenn Sie sich sicher sind, was die Einstellung bewirken. Infolge dieser Einstellungen kann die Schutzfunktion der Firewall vollständig oder teilweise ausgeschaltet werden.

Grundeinstellungen



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Firewall /NAT** und wählen Sie aus dem Untermenü den Eintrag **Grundeinstellungen**.

Hier können Sie **Einwahlfilter** und **Datenfilter** aktivieren und bestimmen, welcher Filtersatz jeweils angewendet wird.

Ein **Einwahlfilter** prüft, ob ein Paket berechtigt ist eine Anwahl auszulösen. Er ist nur aktiv, wenn keine Verbindung zum Internet besteht. Bei bestehender Verbindung zum Internet sind Einwahlfilter unwirksam. Ein **Datenfilter** prüft den Typ eines Datenpaketes und ist nur wirksam, wenn eine Verbindung zum Internet besteht.

Werksseitig sind beide Filter aktiviert.

Einige Online-Spiele nutzen große UDP-Pakete zur Übertragung von Daten. Diese müssen fragmentiert werden, das heisst sie werden in mehrere kleine Pakete aufgeteilt. Die Firewall Ihres Teledat Routers läßt standardmäßig keine fragmentierten UDP-Pakete passieren. Um diese Art von Pakete zu verarbeiten, aktivieren Sie die Option **Pakete annehmen** im Bereich **Fragmentierte UDP-Pakete**. Beachten Sie bitte, dass diese Einstellung die Sicherheit Ihres Teledat Routers beeinträchtigt.

IP-Filter

Für Ihren Teledat Router können Sie bis zu zwölf **Filtersätze** mit jeweils bis zu sieben Regeln definieren. Reichen Ihnen sieben Regeln nicht aus, erstellen Sie einen weiteren Filtersatz und verbinden dann beide Filtersätze über **Verknüpfter Filtersatz**.

Die **Regeln** können positiv oder negativ formuliert werden. Sie können Datenpakete eines bestimmten Typs bewusst passieren lassen oder bewusst blockieren.

Die Filtersätze **Standard-Einwahlfilter** und **Standard-Datenfilter** sind bereits vorkonfiguriert.

Der **Standard-Einwahlfilter** enthält die aktivierte Regel **Block Net Bios**, die alle über den Port 137-139 hereingehenden IP-Pakete blockiert.

Der **Standard-Datenfilter** enthält die aktivierte Regel **xNet Bios->DNS**, die alle über den Port 137-139 herausgehenden IP-Pakete mit dem Zielport 53 blockiert. Zusätzliche Regeln sind vordefiniert, aber **nicht** aktiviert. Sie werden im Folgenden beispielhaft erklärt.

Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Firewall/NAT**. Wählen Sie aus dem Untermenü den Eintrag **IP-Filter**.

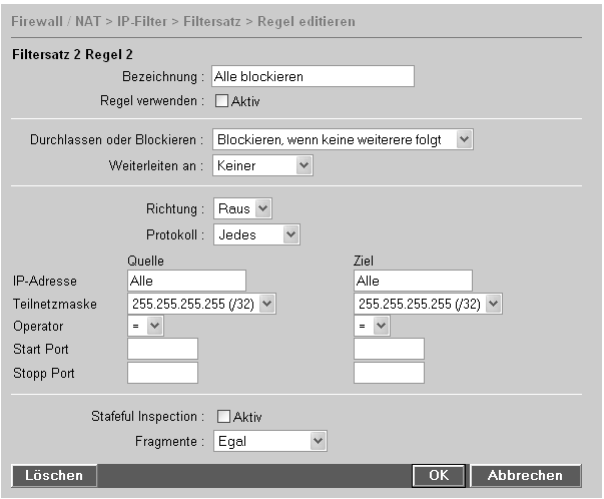
Um einen Filtersatz zu bearbeiten, wählen Sie den zugehörigen Eintrag (Standard-Datenfilter) unter **Bezeichnung**.

Klicken Sie auf den Button **Löschen**, werden alle benutzerdefinierten Einstellungen gelöscht. Die Filtereinstellungen entsprechen dann wieder den Werkseinstellungen.

Hier sind die einzelnen Regeln des Filtersatzes aufgeführt.

Unter **Bezeichnung** wird der frei wählbare Name des Filtersatzes angegeben. Ein Haken bei **Aktiv** kennzeichnet eine aktive Regel.

Öffnen Sie die zweite Regel durch einen Klick auf die zugehörige Bezeichnung (**Alle blockieren**).



In diesem Fenster wird die Regel definiert.

Unter **Bezeichnung** ist der frei wählbare Name der Regel angegeben.

Soll die Regel angewandt werden, setzen Sie einen Haken vor **Aktiv** bei **Regel verwenden**. Dies ist der gleiche Haken, den Sie in der Übersicht des Filtersatzes setzen oder löschen können.

Die gezeigten Einstellungen für die Regel **Alle blockieren** bewirken, dass alle herausgehende Pakete mit beliebiger Quelle und Ziel blockiert werden, wenn sie Folgeregeln nicht erfüllen.

Für die Option **Durchlassen oder Blockieren** gelten folgende Einstellungen:

- **Durchlassen**: Ist die Regel erfüllt, darf das Datenpaket passieren.
- **Blockieren**: Ist die Regel erfüllt, wird das Paket gestoppt
- **Durchlassen, wenn keine weitere folgt:** Wenn das Datenpaket diese, aber keine der folgenden Regeln in diesem Filtersatz erfüllt, darf es passieren.
- **Blockieren, wenn keine weitere folgt:** Wenn das Datenpaket diese, aber keine der folgenden Regeln in diesem Filtersatz erfüllt wird, wird es gestoppt.

Unter **Weiterleiten an** können Sie einen weiteren Filtersatz zur Prüfung des Datenpaketes angeben.

Mit der **Richtung** bestimmen Sie, ob die Regel für ein abgehendes (**Raus**), oder für ein ankommendes (**Rein**) Datenpaket gültig ist. Wählen Sie das **Protokoll** aus, für welches die Regel gelten soll. Wählen Sie zum Beispiel TCP, wenn nur TCP-Pakete durch die Regel geprüft werden sollen.

Die **Quelle** gibt an, für welchen Rechner die Regel gilt. Möchten Sie einen einzelnen Rechner angeben, tragen Sie dessen IP-Adresse und die Teilnetzmaske ein. Belassen Sie dagegen den Eintrag **Alle** bei IP-Adresse und geben nur die Teilnetzmaske an, dann gilt die Regel für alle Rechner im Teilnetz.

Unter **Ziel** können Sie die Zieladressen unter Angabe von IP-Adresse und Teilnetzmaske einschränken. Wenn Sie hier das Ziel **Alle** angeben, gilt die Regel für alle Zieladressen; die Teilnetzmaske hat in diesem Fall keine Bedeutung.

Sowohl für Quelle als auch Ziel können Sie als Einschränkungskriterien **Start** und **Stopp-Port** eintragen.

Tipp

Achten Sie darauf, dass Sie bei Protokoll nicht **Jedes** anwählen, denn dann kann der Router die Start und Stopp-Ports nicht speichern. Nach Klick auf **OK**, erscheint in diesem Fall zwar keine Fehlermeldung, die Werte für die Ports werden aber nicht übernommen.

Aktivieren Sie die Option **Stateful Inspection**, werden die Datenpakete auf Anwendungsebene analysiert. Dadurch wird sichergestellt, dass nur angeforderte Datenpakete die Firewall passieren. Dies setzt voraus, dass bei **Protokoll** ein bestimmter Protokolltyp ausgewählt wird (zum Beispiel TCP).

Im Feld **Fragmente** können Sie angeben, ob die Regel unabhängig von der Fragmentierung ist (**Egal**), nur **Unfragmentierte** oder **Fragmentierte** Pakete betrifft oder nur bei Paketen angewandt wird die **zu klein** sind, um einen kompletten Header zu besitzen.

Speichern Sie Ihre Eingaben mit **OK**.

Die weiteren Regeln des **Standard Datenfilters** lassen Datenpakete passieren, die bestimmte Bedingungen erfüllen:

- **DNS Anfragen**: erlaubt herausgehende Anfragen an den Zielport 53 (DNS)
- **HTTP Anfragen**: erlaubt herausgehende Anfragen an den Zielport 80 (HTTP) und somit das Surfen im Internet
- **Mail empfangen**: erlaubt herausgehende Anfragen an den Zielport 110, und somit das Empfangen von E-Mails
- **Mail senden**: erlaubt herausgehende Anfragen an den Zielport 25, und somit das Senden von E-Mails
- **Ping erlauben**: erlaubt herausgehende Anfragen über das Protokoll ICMP

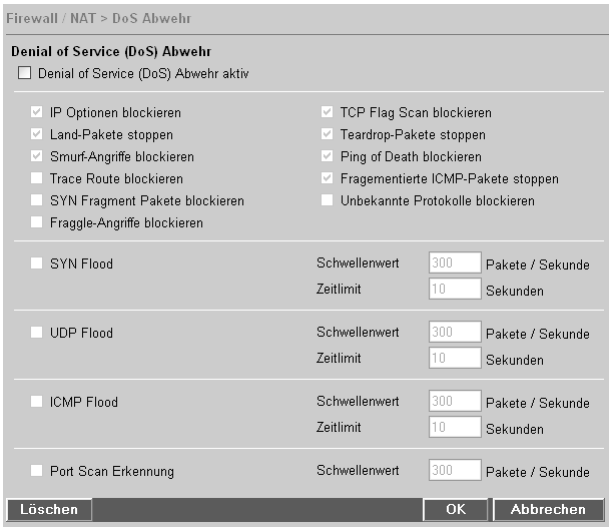
Möchten Sie eine oder mehrere dieser Regeln anwenden, so setzen Sie jeweils einen Haken vor **Aktiv** bei **Regel verwenden** im jeweiligen Profil oder nehmen Sie die Aktivierung in der Profilübersicht vor.

Möchten Sie zum Beispiel die Internetaktivitäten auf das Surfen im Internet beschränken, ist es notwendig die Regeln **Alle blockieren**, **DNS Anfragen** und **HTTP Anfragen** zu aktivieren.

DoS Abwehr

Denial of Service(DoS)-Angriffe zielen darauf, einen Server durch Überlasten mit IP-Paketen lahmzulegen. Die DoS-Funktion Ihres Teledat Routers erlaubt es, diese Angriffe abzufangen beziehungsweise die Wirkung abzumildern und erkannte Angriffe über SysLog (siehe Seite 58) zu melden.

Mit der DOS-Abwehr verfügt Ihr Teledat Router über eine sehr leistungsstarke Funktion, um die Verfügbarkeit von Internet-Diensten (zum Beispiel Web-Server) zu erhöhen. Da diese Funktion Rechenleistung Ihres Teledat Routers bindet, sollten Sie die DOS-Abwehr nur dann aktivieren, wenn Sie Internetdienste anbieten.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Firewall/NAT** und wählen Sie aus dem Untermenü den Eintrag **DoS Abwehr**.

Um die DoS-Abwehr zu aktivieren, setzen Sie den Haken vor **Denial of Service (DoS) Abwehr aktiv**.

Wählen Sie jetzt die Angriffe aus, die überwacht und protokolliert werden sollen, indem Sie jeweils einen Haken davor setzen.

Klicken Sie auf **Löschen**, werden alle benutzerdefinierten Einstellungen wieder auf die Werkseinstellungen zurückgesetzt.

Ist **IP Optionen blockieren** aktiv, stoppt der Router alle IP-Pakete, deren Header Optionen enthalten. Das können zum Beispiel Routinginformationen sein. Werden IP-Pakete mit derartigen Optionen weitergeleitet, können damit Angaben zur Netzwerkstruktur hinter einer Firewall weitergegeben werden.

Land-Pakete stoppen bedeutet, dass der Router keine SYN-Pakete annimmt, deren Absender- und Empfängeradressen übereinstimmen. Einige ältere Systeme kommen damit nicht zurecht und stürzen ab oder rebooten.

Bei einem **Smurf Angriff** sendet der Angreifer andauernd ICMP Echo Request (Ping) Pakete an die Broadcast Adresse eines Netzwerkes, wodurch alle Rechner dieses Netzwerkes ein ICMP Echo Reply Paket an die Source Adresse senden. Der Angreifer muss somit nur die IP des Zielrechners als die Source Adresse in die Pakete schreiben um dessen Netzwerkverbindung zu überlasten. Unter **Smurf Angriffe blockieren** ist zu verstehen, dass der Router alle ICMP Pings ignoriert, die auf seine Broadcast-Adresse gerichtet sind.

Ist die Option **Trace Route blockieren** gesetzt, leitet der Router keine Trace Route Pakete weiter.

SYN Fragment Pakete blockieren heißt: TCP SYN Frames mit gesetztem More-Flag werden blockiert.

Durch das Stoppen ankommender Broadcast UDP-Pakete, werden **Fraggle Angriffe** verhindert.

Durch **TCP Flag Scan blockieren** werden TCP/IP Pakete mit regelwidrig gesetzten Flags gestoppt. Mit Hilfe derartiger Pakete versuchen Angreifer eine Sicherheitslücke zu öffnen.

Indem Sie die Option **Teardrop-Pakete stoppen** aktivieren, wehren Sie Teardrop-Angriffe ab. Ein solcher Angriff nutzt einen Fehler in älteren Windows Versionen (Win95, NT4) beim Zusammenfügen von IP Paket Fragmenten. Beim Eintreffen von Fragmenten werden bei allen Fragmenten (außer dem ersten) die IP Header entfernt und die Nutzdaten zusammengefügt. Bei der Teardrop Attacke werden falsche Fragment Offset Werte benutzt, um das folgende Pakete vollständig in das vorhergehende Paket zu ‚integrieren'. Dadurch wird der Kopierfunktion ein negativer Wert übergeben (zu kopieren = end – offset). Da die Kopierfunktion aber ein ‚unsigned integer' erwartet, wird dadurch möglicherweise – je nach IP Implementation der Stack überschrieben, was wiederum zum Absturz des IP Moduls oder des ganzen Systems führt.

Ping of Death blockieren: damit werden Pakete mit überhöhter oder regelwidriger Größe gestoppt. Bei einem solchen Angriff sendet der Angreifer ein überlanges ICMP Echo Request Paket (größer als 65536 Bytes), das zu einem Überlauf des Buffers für IP Pakete und somit zum Absturz oder Reboot des Rechners führen kann.

Fragmentierte ICMP-Pakete stoppen wird aktiviert, um ICMP Frames mit gesetztem More-Flag zu stoppen.

Um IP-Pakete mit nicht-definiertem Protokolltyp zu blockieren, versehen sie die Option **Unbekannte Protokolle blockieren** mit einem Häkchen.

Aktivieren Sie **SYN Flood**, **UDP Flood** beziehungsweise **ICMP Flood**, geben Sie jeweils die Anzahl der Pakete pro Sekunde als **Schwellenwert** und die Sekunden als **Zeitlimit** an. Die Annahme weiterer SYN, UDP beziehungsweise ICMP Pakete wird verweigert, wenn die Zahl der innerhalb des eingetragenen Zeitlimits eintreffenden Pakete den Schwellenwert übersteigt.

Das Minimum für das Zeitlimit beträgt 5 Sekunden. Der Schwellenwert muss größer als 150 sein.

Bei einem **SYN Flood** Angriff schickt der Angreifer IP Pakete mit falscher Absenderadresse (Spoofed IPs) und gesetztem SYN Flag. Dadurch wird dem Zielrechner ein Verbindungsaufbau vorgetäuscht und der Zielrechner schreibt einen Eintrag in seine Connection Table. Falls nun die Connection Table voll ist, werden keine neuen Verbindungen mehr angenommen und echte Verbindungen zurückgewiesen bis wieder Platz in der Connection Table ist. Der **UDP Flood** Angriff basiert weitgehend auf dem Smurf Angriff (siehe oben), nur werden bei diesem Angriff UDP Pakete verwendet. Bei einem **ICMP Flood** Angriff sendet der Angreifer ICMP Pakete und überlastet die Netzwerkverbindung des Ziels (dazu muss der Angreifer natürlich mehr Bandbreite als das Ziel haben).

Aktivieren Sie **Port Scan Erkennung**, um die PortScans zu protokollieren, die die unter **Schwellenwert** angegebene Geschwindigkeit übertreffen. Der Schwellenwert muss hier ebenfalls größer als 150 sein. Mit Hilfe eines Port-Scan versucht ein Angreifer herauszufinden welche Ports aktiv sind, das heisst welche Dienste dieser spezielle Rechner anbietet. Diese Dienste können ausgenutzt werden, um in das System einzudringen.

Bitte aktivieren Sie abschliessend Ihre Einstellungen mit **OK**.

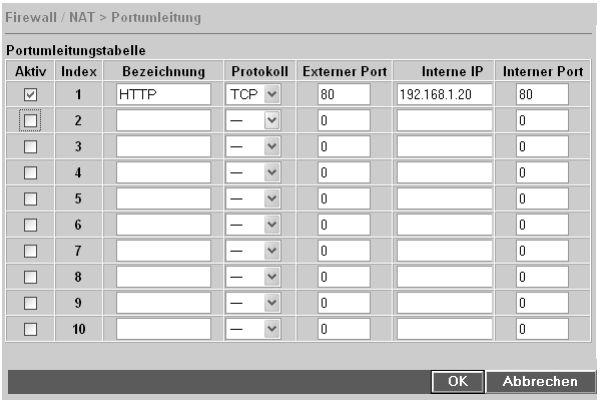
Portumleitung

In diesem Abschnitt wird gezeigt, wie Sie den Zugriff auf bestimmte Dienste auf Rechnern des eigenen Netzwerks für beliebige Rechner aus dem Internet ermöglichen.

Ihr Teledat Router ist im Internet nur über eine einzige IP-Adresse erreichbar. Daher wird ein Port der Router IP-Adresse fest mit einem bestimmten Port eines Rechners im internen Netzwerk verbunden. Nun ist der Rechner im hausinternen Netz direkt für Nutzer des externen Netzwerks zugänglich.

!

Hacker können in diesem Stadium aus der offenen Tür eine Sicherheitslücke machen. Stellen Sie daher sicher, dass ein aus dem Internet erreichbarer Rechner keine Administrationsfunktionen für das restliche Netzwerk ausübt und auch keine aktiven (oder aktivierbaren!) Verbindungen zu anderen Rechnern im internen Netz hat. Stattdessen sollte die Verbindung zu einer bestimmten Anwendung führen, die zulässige Zugriffe sinnvoll bearbeitet und unzulässige Verbindungen abblockt. Weiterhin sollten sich keine wichtigen hausinternen Daten auf einem solchen Rechner befinden.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Firewall/NAT** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Portumleitung**.

Sie können bis zu zehn Portumleitungen definieren.

Ein Haken unter **Aktiv** kennzeichnet eine aktive Portumleitung.

Vergeben Sie unter **Bezeichnung** einen frei wählbaren Namen für die Portumleitung.

Wählen Sie in der nächsten Spalte das **Protokoll** aus, welches Ihre Anwendung benutzt. Einige Anwendungen nutzen UDP und TCP. In diesem Fall nehmen Sie einen Eintrag für UDP und einen Eintrag für TCP vor.

Tragen Sie unter **Externer Port** den Port ein, den die Software des externen Benutzers aus dem Internet anwählen muss. Dieser wird dann auf einen Rechner im internen Netz umgeleitet. Die **Interne IP** gibt die IP-Adresse des Rechners in Ihrem Netzwerk an, der aus dem Internet angewählt werden soll.

Tipp

Rechnern mit Portumleitung sollten Sie eine feste IP-Adresse innerhalb Ihres LAN zuweisen. Nur dann ist gewährleistet, dass die Verbindung mit dem Port des Teledat Routers immer korrekt funktioniert. Wird eine Portumleitung für einen DHCP-Client konfiguriert, kann dessen IP-Adresse wechseln. Somit ist nicht gewährleistet, dass die Portumleitung immer korrekt funktioniert.

Unter **Interner Port** geben Sie bitte den Port an, auf welchem der Rechner seinen Dienst anbietet.

Die Abbildung zeigt ein Beispiel für eine Portumleitung: der interne Rechner mit der IP-Adresse 192.168.1.20 soll als Web-Server genutzt werden. Alle Anfragen, die der Router über den Port 80 erhält, werden an den angegebenen Rechner weitergeleitet.

!

Bitte beachten Sie, dass mit dieser Einstellung eine Fernwartung über den ab Werk eingestellten Port 80 nicht mehr möglich ist. Die Portumleitungstabelle hat eine höhere Priorität als die Einstellung unter Fernwartung. Möchten Sie die Fernwartungsoption nutzen, ändern Sie bitte in diesem Fall den Port für die Fernwartung.

Tipp

Sie können abweichend von der üblichen Konvention einen anderen öffentlichen Port für den Dienst HTTP definieren. Dieser Port muss dann explizit angegeben werden, da üblicherweise Port 80 angesprochen wird. Haben Sie beispielsweise den Port 4500 als öffentlichen Port eingegeben und Ihr Teledat Router hat vom ISP die IP-Adresse http://62.158.247.134 erhalten. In Ihrem Webbrowser tragen Sie nun 62.158.247.134:4500 ein.

Ist Ihr lokaler Webserver in Ihrem LAN gestartet, benötigt der gewünschte Besucher aus dem Internet die IP-Adresse des Teledat Routers. Die IP-Adresse wird im Menü **Home** angezeigt (siehe Seite 17).

Tipp

In der Regel wird die IP-Adresse dynamisch vergeben. Wird die Verbindung wegen Inaktivität abgebaut, wird bei erneuter Anwahl eine neue IP-Adresse vergeben. Bei den meisten Pauschaltarifen (Flatrate) erfolgt einmal pro Tag ein Wechsel der IP-Adresse. Koppeln Sie daher die dynamisch vergebene IP-Adresse über einen entsprechenden Dienstanbieter mit einem Hostnamen (siehe Seite 54).

!

Es ist nicht möglich, die Portumleitung aus dem internen Netz heraus zu testen!

Portöffnung

Die NAT-Funktion schützt oder verhindert den Zugriff auf bestimmte Ports eines Rechners hinter dem NAT-Schutzschild des Routers. Das ist aber nicht immer gewünscht. Für viele Anwendungen (Netmeeting, Quake, Streaming Video, QuickTime, etc.) ist ein ganzer Portbereich für die Datenübertragungen vorgesehen. In diesen Fällen ist es notwendig, einen ganzen Portbereich zu öffnen.

Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Firewall/NAT** und wählen Sie aus dem Untermenü den Eintrag **Portöffnung**.

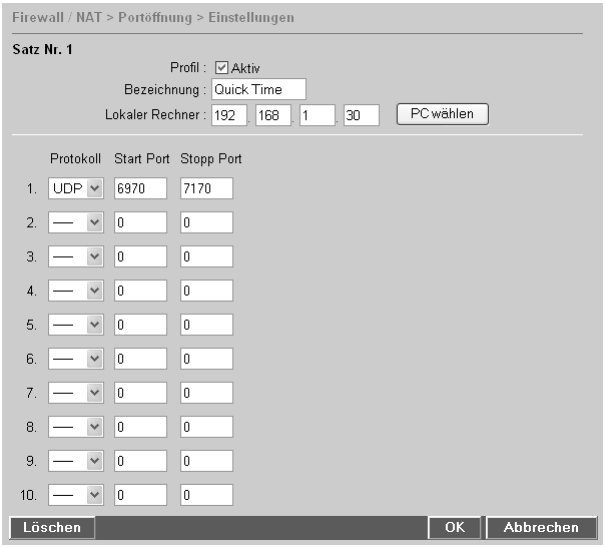
Auf dieser Konfigurationsseite werden die bestehenden **Portöffnungen** aufgelistet.

Klicken Sie auf **Löschen**, werden alle definierten Portöffnungen gelöscht.

Sie können bis zu zehn offene Portbereiche definieren. In der Übersicht werden zu jeder Portöffnung **Status**, **Index**, **Bezeichnung** und die **Lokale IP-Adresse** angezeigt.

Der Eintrag **Aktiv** unter **Status** weist auf eine aktive Portöffnung hin.

Klicken Sie auf den ersten freien Eintrag unter **Bezeichnung**, um einen offenen Portbereich anzulegen.



In diesem Fenster nehmen Sie die Einstellungen zur Portöffnung vor.

Damit das **Profil** wirksam wird, setzen Sie einen Haken vor **Aktiv**. Vergeben Sie unter **Bezeichnung** einen frei wählbaren Namen für das Profil.

Tragen Sie anschließend unter **Lokaler Rechner** die IP-Adresse des Rechners ein, an den die Daten weitergeleitet werden sollen.

Im nächsten Schritt wählen Sie das **Protokoll** aus und tragen **Start** und **Stopp Port** ein. Sie können bis zu zehn verschiedene Portbereiche angeben.

Speichern Sie Ihre Einstellung durch Klick auf **OK**.

Das Beispiel zeigt eine Portöffnung für eine QuickTime Streaming Verbindung. Über QT-Streaming lassen sich Video und Audiodaten per Internet anschauen. Die Datenquelle sendet einen Datenstrom aus (Strom = engl. Stream). In diesen Strom klinkt sich jetzt der QT-Player ein. Die Übertragung des Datenstroms kann über den üblichen HTTP-Port 80 erfolgen. Diese Verbindung ist aber recht langsam. Das wiederum führt zu Einbußen in der Qualität. Eine bessere Übertragungsleistung wird über einen UDP-Port erreicht, wobei die Daten auf verschiedene Ports aufgeteilt werden. Der Client erwartet Daten über UDP zwischen den Ports 6970 und 7170. Das NAT-Routing vom Teledat Router verhindert aber, dass die Daten zum QT-Rechner durchgelassen werden. Mit den oben gezeigten Einstellungen werden alle UDP-Daten, welche für den Portbereich 6970 bis 7170 bestimmt sind, auf den Rechner mit der angegebenen IP-Adresse weitergeleitet. Welche Ports von Ihren Anwendungen genutzt werden, entnehmen Sie bitte der jeweiligen Dokumentation.

DMZ

Die DMZ-Funktion ist die konsequente Weiterführung der Funktionen Portumleitung und Portbereich öffnen. DMZ ermöglicht das Freischalten aller Ports für einen bestimmten hausinternen Rechner. Das bedeutet, dass alle Anfragen an Ports, welche nicht in der Routingtabelle hinterlegt sind, 1:1 an den DMZ-Rechner weitergeleitet werden. Ein DMZ-Rechner gilt als ungeschützt (entmilitarisiert) - auch wenn er im ansonsten geschützten internen Bereich betrieben wird. Die DMZ-Funktion wird in der Regel für einen internen Internet-Server verwendet.

Klicken Sie in der Menüleiste Ihres Teledat Routers auf **Firewall/NAT** und wählen Sie aus dem angezeigten Untermenü den Eintrag **DMZ** aus.

Damit der **DMZ Rechner** genutzt werden kann, setzen Sie einen Haken vor **Aktiv**.

Tragen Sie unter **Lokale IP** die IP-Adresse des gewünschten DMZ-Rechners ein. Alternativ können Sie auch auf **PC wählen** klicken. Es erscheint eine Liste der verfügbaren Rechner. Selektieren Sie Ihren gewünschten Rechner aus der Liste.

Bestätigen Sie Ihre Eingaben mit **OK**.

Tipp

Haben Sie unterschiedliche Rechner für Portumleitung, Portöffnung und DMZ eingerichtet, erfolgt die Weiterleitung der Anfragen nach folgender Priorität:

1. Ist für den angesprochenen Port eine Portumleitung aktiv, geht das Paket an den dafür angegebenen Rechner.
2. Ist für den angesprochenen Port die Portumleitung nicht aktiv und liegt der Port in einem geöffneten Portbereich, geht das Paket an den dafür angegebenen Rechner.
3. Ist für den angesprochenen Port weder eine Portumleitung aktiv noch ein Portbereich geöffnet, wird das Paket an den DMZ-Rechner weitergeleitet.

VPN / Routing

Die Funktion VPN ermöglicht den Aufbau einer Verbindung zwischen zwei lokalen Netzwerken über das Internet. Die Verbindung zum entfernten Router wird vom Teledat Router automatisch aufgebaut, wenn eine Adresse in dem jeweils entfernten Netz angewählt wird. Über Ihren Teledat Router kann auch eine Verbindung von einem externen Nutzer zu Ihrem lokalen Netzwerk aufgebaut werden.

Zugangskontrolle

Auf dieser Konfigurationsseite legen Sie die Kriterien für die Einwahl in Ihren Teledat Router fest.

Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **Zugangskontrolle**.

Aktivieren Sie hier die gewünschten Einwahlmöglichkeiten.

Für die Einwahl stehen die Protokolle **PPTP**, **IPSec** und **L2TP** zur Verfügung.

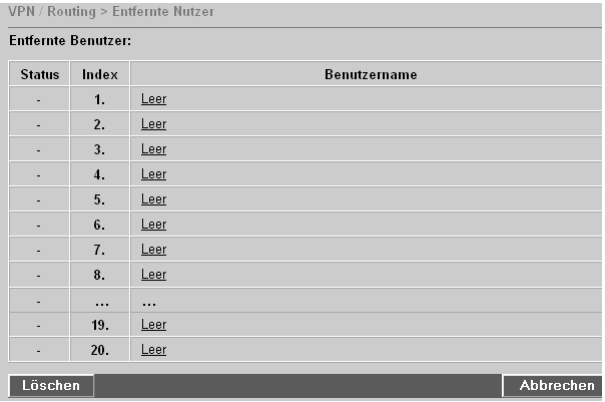
!

Aktivieren Sie alle Protokolle, die für VPN-Verbindungen in die eine oder in die andere Richtung genutzt werden sollen. Ist hier ein Protokoll deaktiviert, kann keine VPN Verbindung mit einem solchen Protokoll hergestellt werden. Dies gilt sowohl für einen Anrufer als auch für einen Anwender im Netzwerk des Routers.

Tipp

Wenn Sie zum Beispiel einen VPN-Server in Ihrem LAN und Ihren Teledat Router für **VPN Pass Through** nutzen möchten, dass heisst lediglich zum Durchleiten der Verbindung, deaktivieren Sie bitte alle VPN-Protokolle.

Entfernte Nutzer

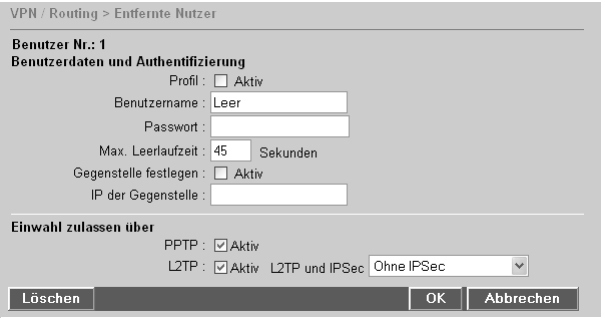


Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **Entfernte Nutzer.**

Sie können hier bis zu 20 Profile für externe Nutzer hinterlegen.

Um ein neues Benutzerprofil einzurichten, wählen Sie ein freies Profil aus der Liste.

Öffnen Sie es durch Klick auf die Bezeichnung in der Spalte **Benutzername**. Der Benutzername ist in der Regel mit der Bezeichnung **Leer** vorbelegt. Haben Sie ein neues Profil angelegt und gespeichert, erscheint der eingetragene Benutzername als Bezeichnung in der Profilübersicht.



Hier legen Sie die Eigenschaften für das neue Profil fest.

Damit das **Profil** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Tragen Sie **Benutzername** und **Passwort** für die Einwahl ein.

Eine Verbindung mit dem externen Nutzer wird nur dann angenommen, wenn er sich durch die hier festgelegten Daten identifizieren kann.

Geben Sie bitte die **Max. Leerlaufzeit** an. Werden innerhalb der hier eingestellten Zeit keine Daten übertragen, wird die Verbindung automatisch abgebaut.

Wird die Option **Gegenstelle festlegen** aktiviert, muss der externe Benutzer seine IP-Adresse (PPTP oder L2TP) übertragen. Diese wird dann mit dem unter **IP der Gegenstelle** eingetragenen Wert verglichen. Nur wenn die Angaben übereinstimmen, wird die Einwahl gewährt.

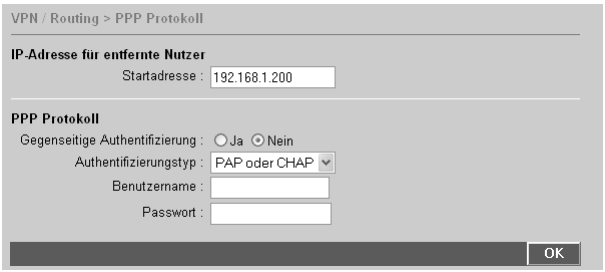
Unter **Einwahl zulassen über** wählen Sie die Protokolle aus, über die eine Einwahl erfolgen kann.
Speichern Sie Ihre Eintragungen mit **OK**.

Tipp

Bei VPN Verbindungen benötigt der einwählende Rechner die IP-Adresse des Routers im Internet. In der Regel wird die IP-Adresse dynamisch vergeben. Wird die Verbindung des Routers zum Internet wegen Inaktivität abgebaut, erhält er bei erneuter Anwahl eine neue IP-Adresse. Bei den meisten Pauschaltarifen (Flatrate) erfolgt einmal pro Tag ein Wechsel der IP-Adresse. Um den Router dennoch im Internet zu erreichen, sollten Sie die dynamisch vergebene IP-Adresse über einen entsprechenden Dienstanbieter mit einem Hostnamen koppeln (siehe Seite 54).

PPP Protokoll

Auf dieser Seite können Sie die IP-Adresse für externe Nutzer und die **Gegenseitige Authentifizierung** konfigurieren.



Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **PPP Protokoll**.

Geben Sie unter **Startadresse** die IP-Adresse an, die an den ersten externen Nutzer vergeben wird.

Ein weiterer externer Nutzer erhält die auf diese Startadresse folgende IP-Adresse. Sie haben zum Beispiel die 192.168.1.200 als Startadresse angegeben. Dem ersten externen Nutzer wird diese Adresse zugewiesen. Der nächste Nutzer erhält die folgende Adresse 192.168.1.201.

!

Die zu vergebenden Adressen sollten nicht im Adressbereich des DHCP-Servers liegen. Bitte vergewissern Sie sich, dass die IP-Adresse noch nicht in Ihrem Netz vergeben ist und freigehalten wird.

In seltenen Fällen erwartet der Anrufer als zusätzliche Sicherung gegen unbefugten Zugriff, dass sich der angerufene Router auch bei ihm authentifiziert (Gegenseitige Authentifizierung). Aktivieren Sie in diesem Fall die Option **Gegenseitige Authentifizierung**.

Die Verfahren PAP oder CHAP werden akzeptiert. In der Regel können Sie daher unter **Authentifizierungstyp** den Eintrag **PAP oder CHAP** stehen lassen. Nur in Ausnahmefällen ist das Umstellen auf **Nur PAP** nötig.

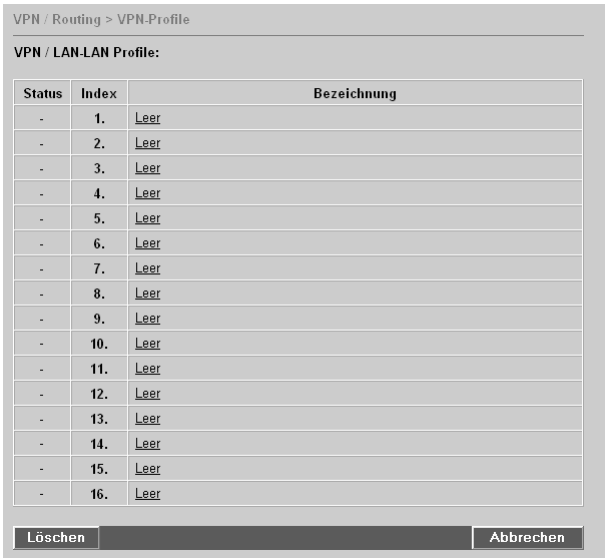
Tragen Sie **Benutzername** und **Passwort** ein. Diese Angaben werden dann vom Teledat Router an den Anrufer zurückgegeben.

Klicken Sie bitte auf **OK**, um Ihre Einstellungen zu speichern.

VPN Profile

In diesem Abschnitt wird beschrieben, worauf bei der Erstellung eines VPN-Profils zu achten ist.

Durch die Vielzahl der Wechselwirkungen zwischen LAN-LAN Verbindungen, Einwahl bei einem ISP und anderen Einstellungen ist die Einrichtung einer VPN-Verbindung sehr komplex. Die Konfiguration eines VPN-Profiles sollten Sie daher nur vornehmen, wenn Sie sich sicher sind, was die Einstellungen bewirken.



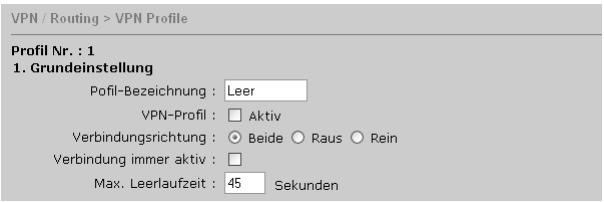
Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **VPN-Profile**.

In dieser Übersicht sind alle Profile aufgelistet. Sie können bis zu 16 verschiedene VPN-Profile einrichten.

Der Eintrag **Aktiv** unter **Status** kennzeichnet ein aktives Profil.

Klicken Sie auf den Button **Löschen**, werden alle benutzerdefinierten Profile gelöscht.

Um ein neues Profil zu erstellen, wählen Sie einen freien Eintrag aus der Liste. Öffnen Sie es durch Klick auf die **Bezeichnung**. Die Bezeichnung ist in der Regel mit **Leer** vorbelegt. Haben Sie ein neues Profil angelegt und gespeichert, erscheint der vergebene Profilname als Bezeichnung in der Profilübersicht.


VPN / Routing > VPN Profile
Profil Nr. : 1
1. Grundeinstellung
Pofil-Bezeichnung : Leer
VPN-Profil : Aktiv
Verbindungsrichtung : Beide Raus Rein
Verbindung immer aktiv :
Max. Leerlaufzeit : 45 Sekunden

In diesem Menü legen Sie die Eigenschaften für das neue Profil fest. Im Folgenden werden die vier einzelnen Menübereiche nacheinander beschrieben.

Im Bereich **Grundeinstellung** sollten Sie im Feld **Profil-Bezeichnung** einen neuen Namen für das Profil vergeben. Damit das **VPN-Profil** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Legen Sie unter der Option **Verbindungsrichtung** fest, in welcher Richtung die VPN-Verbindung aufgebaut werden kann. Die Einstellung **Beide** ermöglicht den Verbindungsaufbau in beiden Richtungen. Wählen Sie die Einstellung **Raus**, kann der lokale Router nur eine Verbindung zu einem anderen Router oder VPN-Server aufbauen; er selber kann nicht angewählt werden. Wählen Sie dagegen **Rein**, nimmt der Router zwar eine Verbindung an, baut aber selber keine auf.

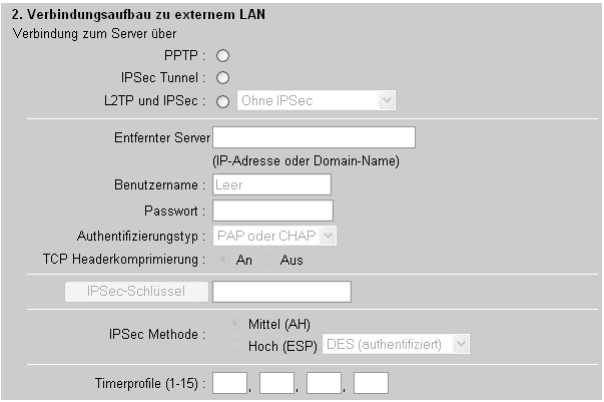
Diese Festlegung der Verbindungsrichtung gilt nur für den Aufbau der Verbindung. Ist eine Verbindung einmal aufgebaut, können unter Umständen die Netzwerke beider Router aufeinander zugreifen!

Wenn Sie neben die Option **Verbindung immer aktiv** den Haken setzen, baut Ihr Teledat Router automatisch eine VPN-Verbindung auf, sobald eine Internetverbindung besteht. Wird die VPN-Verbindung bei bestehender Internetverbindung unterbrochen, erfolgt umgehend ein Neuaufbau.

Die Option **Verbindung immer aktiv** bedingt als **Verbindungsrichtung** die Einstellung **Raus**. Sollten Sie dort vorher eine abweichende Auswahl getroffen haben, wird diese automatisch auf diesen Wert umgestellt.

Soll Ihr VPN-Netzwerk immer aktiv sein, muss auch die Internetverbindung ständig aufrechterhalten werden.

Soll die Verbindung nicht dauernd aktiv sein, geben Sie bitte die **Max. Leerlaufzeit** an. Werden innerhalb der hier eingestellten Zeit keine Daten übertragen, wird die Verbindung automatisch abgebaut.



Der zweite Bereich ist für die Festlegung der Eigenschaften für den **Verbindungsaufbau zu externem LAN** vorgesehen.

Legen Sie unter **Verbindung zum Server über** fest, wie die VPN Verbindung aufgebaut werden soll. Hier stehen die Protokolle **PPTP**, **IPSec Tunnel** und **L2TP** zur Verfügung.

Tipp

Wir empfehlen Ihnen, bei Ihren ersten Tests mit VPN das Protokoll PPTP zu verwenden. PPTP ist die einfachste VPN-Option.

Das Protokoll **L2TP** erlaubt es Ihnen, IPSec als Option zu setzen. Sie können wählen zwischen den Einstellungen **ohne IPSec**, **IPSec, wenn verfügbar** (IPSec, wenn die Gegenstelle das unterstützt) und **Nur IPSec** (Gegenstelle muss IPSec unterstützen).

Identifizieren Sie den **Entfernten Server** durch Angabe von dessen **IP-Adresse oder Domain-Name**. Sie können die IP-Adresse, den Domain-Namen oder die DDNS-Adresse des entfernten Routers oder VPN-Servers eintragen.

Geben Sie unter **Benutzername** und **Passwort** Ihre Daten für die PPP-Authentifizierung ein.

!

Nur wenn Ihre Daten korrekt sind und mit den Angaben bei der Gegenstelle übereinstimmen, ist eine Einwahl in das entfernte Netz beziehungsweise den entfernten Router möglich.

Die Verfahren PAP oder CHAP werden akzeptiert. In der Regel können Sie daher unter **Authentifizierungstyp** den Eintrag **PAP oder CHAP** stehen lassen. Nur in Ausnahmefällen ist das Umstellen auf **Nur PAP** nötig. Bei der Nutzung von IPSec Tunnel ist dieses Feld deaktiviert; die Authentifizierung wird in diesem Fall über den IPSec-Schlüssel vorgenommen.

Die Option **TCP Headerkomprimierung** wird von den meisten Systemen unterstützt, um die Datenübertragung zu beschleunigen. Sie aktivieren diese Funktion, indem Sie den Punkt vor **An** setzen. Bei IPSec Tunnel steht die Option nicht zur Verfügung.

Möchten Sie Ihre VPN-Verbindung über einen **IPSec Tunnel** aufbauen, klicken Sie auf den Button **IPSec-Schlüssel**, um den Schlüssel für die Anwahl des entfernten Routers zu definieren.

Tragen Sie in diesem Fenster den **IPSec-Schlüssel** ein, der bei der Anwahl des entfernten Netzwerkes durch Ihren Teledat Router eingesetzt wird.

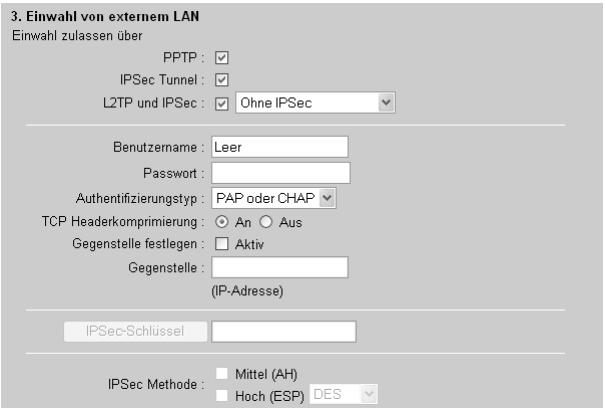
Wiederholen Sie Ihre Eingabe bei **IPSec-Schlüssel bestätigen**. Ihr Teledat Router überprüft, ob die beiden Einträge übereinstimmen. Speichern Sie Ihre Angaben mit **OK**.

Tipp

Sie können für jedes VPN-Profil einen individuellen IPSec-Schlüssel für die Anwahl des entfernten Routers hinterlegen. Nur dann, wenn dieser IPSec-Schlüssel definiert ist, kann die Verbindung mit **IPSec** aufgebaut werden.

Bei einem **IPSec Tunnel** können Sie zwischen zwei Arten der Verbindungssicherung wählen. Die Option **Mittel (AH)** realisiert die Sicherung durch eine Authentifizierung. Wählen Sie **Hoch (ESP)**, können Sie nochmals zwischen einfacher und dreifacher DES-Verschlüsselung mit oder ohne zuätzlicher Authentifizierung wählen.

Über den **Verbindungstimer** können Sie den Router veranlassen, die aktuelle LAN-LAN-Verbindung auf bestimmte Zeiten und Tage zu beschränken. Die Definition der Timereinstellungen nehmen Sie im Menü **Verbindungstimer** im Bereich **Extras** vor (siehe Seite 56). Einem VPN-Profil können Sie bis zu vier **Timerprofile** zuweisen.



Im dritten Bereich können Sie die Eigenschaften für die **Einwahl von externem LAN** definieren.

Legen Sie mit der Option **Einwahl zulassen über** fest, wie der Verbindungsaufbau erfolgen darf.

Sie können zwischen den Protokollen **PPTP**, **IPSec Tunnel** und **L2TP** wählen.

Aktivieren Sie **L2TP**, ist zusätzlich IPSec-Sicherung möglich.

Verbindungen über **IPSec-Tunnel** werden immer unter Verwendung von IPSec aufgebaut. Bei PPTP besteht keine Möglichkeit der IPSec-Sicherung.

Tragen Sie unter **Benutzername** und **Passwort** Ihre Daten für die **PPP-Authentifizierung** ein.

Tipp

Beachten Sie, dass Benutzerkennung und Passwort eindeutig sein müssen. Das heisst, jede Kombination darf nur einmal vergeben werden.

Als Verfahren werden PAP oder CHAP akzeptiert. In der Regel können Sie daher unter **Authentifizierungstyp** den Eintrag **PAP oder CHAP** stehen lassen. Nur in Ausnahmefällen ist das Umstellen auf **Nur PAP** nötig. Bei der Nutzung von IPSec Tunnel ist dieses Feld deaktiviert; die Authentifizierung wird in diesem Fall über den IPSec-Schlüssel vorgenommen.

Die Option **TCP Headerkomprimierung** wird von den meisten Systemen unterstützt, um die Datenübertragung zu beschleunigen. Sie aktivieren diese Funktion, indem Sie den Punkt vor **An** setzen. Bei **IPSec Tunnel** steht die Option nicht zur Verfügung.

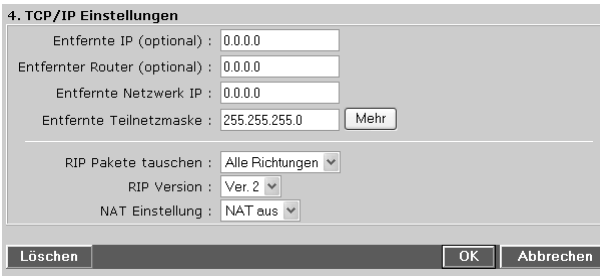
Aktivieren Sie **Gegenstelle festlegen** um sicherzustellen, dass sich nur der Router einwählen kann, dessen IP-Adresse Sie unter **Gegenstelle** eingetragen haben. Stimmt die Angabe des anwählenden Routers nicht mit der eingetragenen überein, wird die Einwahl verweigert.

Im Allgemeinen wird beim Aufbau des IPSec-Tunnels der Schlüssel verwendet, der unter **VPN/Routing –> IKE/IPSec-Schlüssel** definiert wird. Wenn Sie die Gegenstelle festgelegt haben, können Sie für dieses VPN-Profil einen eigenen IPSec-Schlüssel für die Einwahl in den Teledat Router definieren. Klicken Sie dazu auf den Button **IPSec-Schlüssel**.

Tragen Sie in diesem Fenster den **IPSec-Schlüssel** ein, der bei der Einwahl des entfernten Netzwerkes in Ihren Teledat Router eingesetzt werden soll.

Wiederholen Sie Ihre Eingabe bei **IPSec-Schlüssel bestätigen**. Ihr Teledat Router überprüft, ob die beiden Einträge übereinstimmen. Speichern Sie Ihre Angaben mit **OK**.

Bei einem **IPSec Tunnel** können Sie zwischen zwei Arten der Verbindungssicherung wählen. Die Option **Mittel (AH)** realisiert die Sicherung durch eine Authentifizierung. Wählen Sie **Hoch (ESP),** können Sie nochmals zwischen einfacher und dreifacher DES-Verschlüsselung mit oder ohne zuätzlicher Authentifizierung wählen.

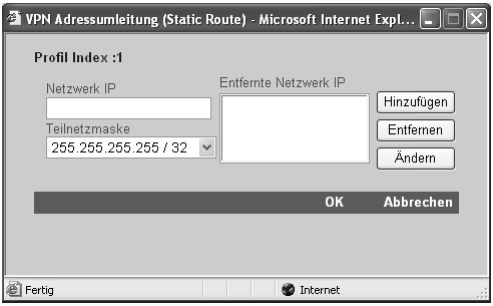


Im vierten Bereich definieren Sie die **TCP/IP-Eigenschaften** Ihrer VPN-Verbindung.

Unter **Entfernte IP** wird die IP-Adresse Ihres Teledat Routers im externen Netzwerk angegeben.

Im Normalfall wird die Adresse von der Gegenstelle automatisch vergeben und Sie können hier den Eintrag **0.0.0.0** übernehmen. Bei **Entfernter Router** kann die IP-Adresse des Routers der Gegenstelle eingetragen werden. In der Regel wird die Adresse automatisch von der Gegenstelle geliefert und es wird **0.0.0.0** eingetragen.

Die Einträge **Entfernte Netzwerk IP** und **Entfernte Teilnetzmaske** legen fest, welche IP-Adressen in dem entfernten VPN-Netz liegen. Wird eine dieser IP-Adressen über den Teledat Router angefragt, baut er automatisch eine Verbindung zum anderen Netz auf. Werden zum Beispiel als Entfernte Netzwerk IP die 192.168.0.0 und als Entfernte Teilnetzmaske der Wert 255.255.255.0 eingetragen bedeutet das: werden Adressen zwischen 192.168.0.1 und 192.168.0.254 angefragt, wird eine Verbindung zum entfernten Netzwerk aufgebaut.



Klicken Sie auf **Mehr**, um mehrere entfernte Netzwerke anzugeben.

Tragen Sie die **Netzwerk-IP** ein und übernehmen Sie diese durch Klick auf **Hinzufügen** in die Liste.

Über **Entfernen** können Sie Einträge aus der Liste löschen.

Speichern Sie Ihre Eingaben mit **OK**.

Um unnötigen Verkehr zu vermeiden, tauschen Router Informationen über die von ihnen verwalteten Netze via RIP aus. Legen Sie mit **RIP Pakete tauschen** fest, ob und wie Sie RIP nutzen möchten. Geben Sie ebenfalls die **RIP-Version** an.

Mit der **NAT-Einstellung** legen Sie fest, ob Daten mit dem entfernten Router über NAT oder direkt ausgetauscht werden. Bei **NAT aus** werden Daten ohne NAT in das andere Netz übertragen. Die einzelnen Rechner im Netzwerk des Teledat Routers sind vom entfernten Netz direkt über die IP-Adresse erreichbar.

In diesem Fall müssen beide Netzwerke überschneidungsfreie IP-Adressbereiche haben.

Die Einstellung **NAT ein** bedeutet, die Daten werden mit NAT in das andere Netz übertragen. Der Router verdeckt seinen Adressbereich gegenüber dem entfernten Netz. Somit kann vom entfernten Netz aus kein Rechner im lokalen Netz des Teledat Routers direkt erreicht werden. Möglich bleibt nur der Zugriff vom Netzwerk des Teledat Routers auf das entfernte Netz.

IKE / IP-Sec-Schlüssel

Mit Hilfe von IPSec können Sie Ihre VPN-Verbindungen absichern.

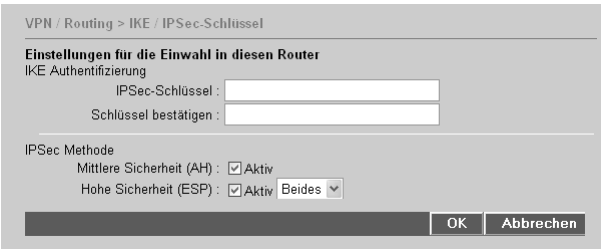
Der IPSec-Schlüssel ermöglicht drei verschiedene Sicherheitsstufen:

- Die Authentifizierung erfolgt über den Schlüssel.
- Die übertragenen Daten werden mit dem Schlüssel codiert.
- Die Authentifizierung und Codierung erfolgen über den Schlüssel.

Sie können auf dieser Konfigurationsseite einen Schlüssel für die Einwahl in diesen Router definieren. Dieser gilt dann für alle VPN-Profile, die über einen IPSec-Tunnel aufgebaut werden und für die in den Profileinstellungen für die **Einwahl von externem LAN** kein eigener Schlüssel definiert wurde.

Tipp

Um IPSec für den Verbindungsaufbau zu nutzen, muss ein Schlüssel eingetragen werden. Fehlt der Eintrag, kann kein Verbindungsaufbau erfolgen.



Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **IKE/IPSec-Schlüssel**.

Geben Sie unter **IKE Authentifizierung** den **IPSec-Schlüssel** für die Einwahl an.

Wiederholen Sie Ihre Eingabe bei **Schlüssel bestätigen**. Ihr Teledat Router überprüft, ob die beiden Eingaben übereinstimmen.

Unter **IPSec Methode** legen Sie das IPSec-Sicherheitsniveau für die Einwahl fest. Bei der Auswahl **Mittlere Sicherheit (AH)** prüft der Router den IPSec-Schlüssel, welchen der entfernte Router übermittelt.

Wählen Sie **Hohe Sicherheit (ESP)**, können Sie angeben, ob die Verschlüsselungsmethode **DES** (einfache Verschlüsselung), **3DES** (dreifache Verschlüsselung) oder **Beides** (DES oder 3DES) akzeptiert wird.

Speichern Sie Ihre Einstellungen mit **OK**.

Static Route

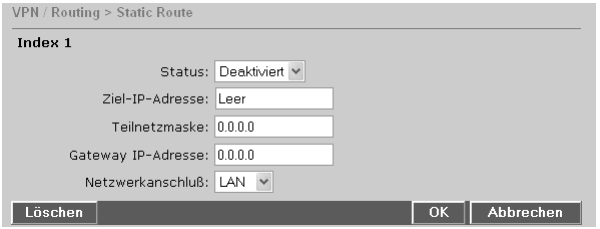
Hier können Sie bis zu zehn Zieladressbereiche festlegen, die in entfernten VPN-Netzwerken erreicht werden können.

Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **Static Route**.

Der Eintrag **Aktiv** unter **Status** kennzeichnet eine aktive Static Route.

Klicken Sie auf den Button **Aktive Routingtabelle zeigen**, um eine Übersicht der aktiven Static Routes zu erhalten (siehe Seite 64).

Um eine neue Static Route festzulegen, klicken Sie auf den ersten freien Eintrag in der Liste. Die Zieladresse ist in der Regel mit **Leer** vorbelegt. Haben Sie ein neues Profil angelegt und gespeichert, erscheint die Zieladresse als Bezeichnung in der Übersicht.



In diesem Menü legen Sie die Eigenschaften für die neue Static Route fest.

Setzen Sie den **Status** auf **Aktiviert**.

Geben Sie **Ziel-IP-Adresse** und **Teilnetzmaske** des entfernten Netzes ein. Im Feld **Gateway IP Adresse** tragen Sie die IP-Adresse des entfernten Gateways ein. Das kann zum Beispiel die IP-Adresse eines entfernten Routers sein. Wählen Sie bei **Netzwerkanschluss** aus, ob sich die entfernte Adresse im **LAN** befindet oder über das **WAN** zu erreichen ist.

Bestätigen Sie abschliessend Ihre Änderungen mit **OK**

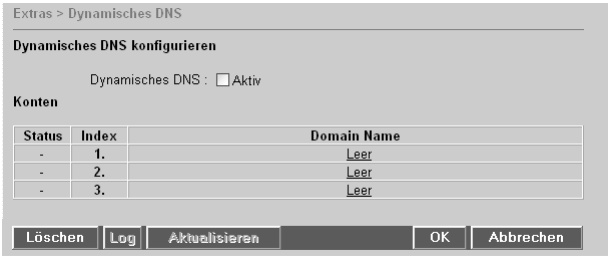
Extras

Dynamisches DNS (DDNS)

Mit Hilfe der Funktion Dynamisches DNS (DDNS) können Sie die Erreichbarkeit Ihres Routers auch unter Verwendung einer wechselnden IP-Adresse sicherstellen. Dem Router wird eine feste URL zugwiesen, die mit der jeweils aktuellen IP-Adresse verknüpft wird. Die Umsetzung erfolgt auf Basis eines voreingestellten DDNS-Dienstes. Sobald sich der Router in das Internet einwählt, wird die aktuell vergebene IP-Adresse an den DDNS-Dienst weitergegeben.

Tipp

In der Regel wird die IP-Adresse von Ihrem ISP dynamisch vergeben. Bei erneuter Anwahl wird eine neue IP-Adresse vergeben. Auch bei den meisten Pauschaltarifen (Flatrate) erfolgt einmal pro Tag ein Wechsel der IP-Adresse. Eine bekannte IP-Adresse ist die Voraussetzung zum Beispiel für eine eigene Webpräsenz. Ansonsten kann keine Auflösung des Namens in die eigentliche IP-Adresse erfolgen. Diese Namensauflösung erledigt der Domain Name Server, kurz DNS. Er übersetzt zum Beispiel die URL <www.Musterfirma.de> in die zugehörige IP-Adresse. Um diese Umsetzung auch mit einer dynamischen IP-Adresse zuverlässig durchzuführen, gibt es spezielle DDNS-Dienste im Internet. Die Anbieter der DDNS-Dienste verknüpfen eine URL mit der jeweils aktuellen IP-Adresse.

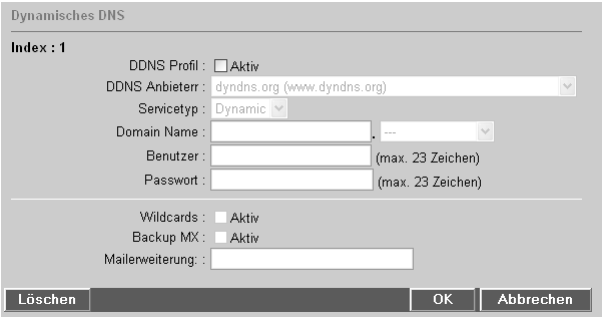


Klicken Sie auf den Eintrag **Extras** in Ihrer Menüleiste und wählen das Untermenü **Dynamisches DNS**.

Damit **Dynamisches DNS** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Klicken Sie auf den Button **Log**, werden die protokollierten DDNS-Aktivitäten angezeigt.

Ihr Teledat Router kann bis zu drei DDNS-Verbindungen verwalten. Der Eintrag **Aktiv** unter **Status** kennzeichnet ein aktives DDNS-Profil. Um ein neues Profil einzurichten, klicken Sie auf den ersten freien Eintrag unter **Domain Name**.



Definieren Sie in diesem Menü die Eigenschaften eines DDNS Profils.

Damit das **DDNS Profil** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Wählen Sie anschließend einen **DDNS-Anbieter** aus der Liste aus.

Die weiteren Optionen sind vom ausgewählten Anbieter abhängig. Nur relevante Optionen werden aktiviert, sodass Sie Ihre Einstellungen vornehmen können.

Wählen Sie zum Beispiel **dyndns.org** als Anbieter, können Sie sich bei **Servicetyp** für **Dynamic**, **Static** oder **Custom** entscheiden. Im Regelfall empfehlen wir die Einstellung **Dynamic** beizubehalten.

Geben Sie im Feld **Domain Name** Ihre URL an. Lautet Ihre DDNS-Adresse **Musterfirma.dyndns.org**, so tragen Sie als Domain Namen **Musterfirma** ein und wählen für die Endung **dyndns.org**.

Bestätigen Sie Ihre Angaben mit **OK**.

Tipp

Vor Verwendung einer DDNS-Adresse müssen Sie diese bei dem jeweiligen DDNS-Anbieter anmelden. Die Web-Adresse des DDNS-Anbieters stimmt in der Regel mit dem Hauptteil der dynamischen Adresse überein (zum Beispiel dyndns.org).

!

Da die Deutsche Telekom nicht Anbieter dieser DDNS-Dienste ist, kann Sie keine Gewähr für deren Verfügbarkeit übernehmen.

Verbindungstimer

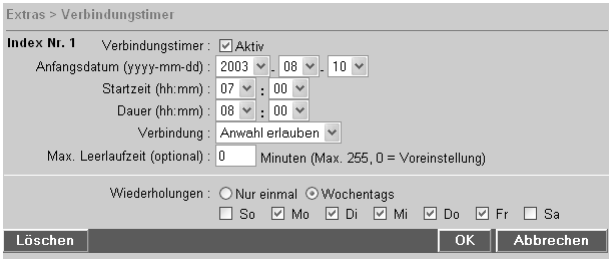
Der Verbindungstimer erlaubt in Verbindung mit der Systemzeit einen automatischen Statuswechsel einzelner Verbindungen. Sie können zum Beispiel die Anwahl nur von Montag bis Freitag ab 7:00 Uhr für die Dauer von 8 Stunden erlauben (siehe untere Abbildung).

Klicken Sie auf den Eintrag **Extras** Ihrer Menüleiste und wählen das Untermenü **Verbindungstimer**.

Sie können hier bis zu 15 Einstellungen definieren.

Der Eintrag **Aktiv** unter **Status** kennzeichnet einen aktiven Verbindungstimer.

Klicken Sie auf den entsprechenden Wert unter **Index**, um das Fenster für die Timerkonfiguration zu öffnen.


Extras > Verbindungstimer
Index Nr. 1
Verbindungstimer : Aktiv
Anfangsdatum (yyyy-mm-dd) : 2003 - 08 - 10
Startzeit (hh:mm) : 07 : 00
Dauer (hh:mm) : 08 : 00
Verbindung : Anwahl erlauben
Max. Leerlaufzeit (optional) : 0 Minuten (Max. 255, 0 = Voreinstellung)
Wiederholungen : Nur einmal Wochentags
So Mo Di Mi Do Fr Sa
Löschen
OK
Abbrechen

In diesem Menü können Sie eine Timereinstellung konfigurieren.

Damit der **Verbindungstimer** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Geben Sie **Anfangsdatum**, **Startzeit** und **Dauer** für den Verbindungsaufbau an. Beachten Sie dabei das jeweils in Klammern vorgegebene Eingabeformat.

Die Einstellung unter **Verbindung** definiert den Status der Verbindung für die im Profil festgelegte Zeit. Geben Sie an, ob Sie eine Verbindung **Aufbauen** oder **Beenden** beziehungsweise die **Anwahl erlauben** oder die **Anwahl sperren** möchten.

Sie können unter **Max. Leerlaufzeit** eine speziell für diese Timereinstellung gültige Festlegung treffen. Werden innerhalb der hier eingestellten Zeit keine Daten übertragen, wird die Verbindung automatisch beendet. Tragen Sie 0 (Null) ein, so gilt die in den Verbindungseinstellungen definierte Zeit.

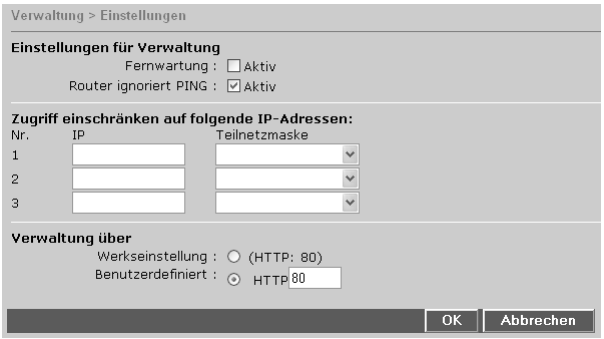
Unter **Wiederholungen** legen Sie fest, ob Ihr Profil **nur einmal** oder an verschiedenen **Wochentagen** gültig ist. Haben Sie **Wochentags** gewählt, setzen Sie vor die betreffenden Tage einen Haken.

Sichern Sie Ihre Einstellungen mit **OK**.

Verwaltung

Einstellungen

Mit diesen Einstellungen können Sie den **Zugriff** auf Ihren Teledat Router regeln.



Klicken Sie auf den Eintrag **Verwaltung** in der Menüleiste und wählen das Untermenü **Einstellungen**.

Aktivieren Sie die **Fernwartung**, um die Konfiguration Ihres Teledat Routers über das Internet zu erlauben.

!

Haben Sie die Fernwartung aktiviert, kann Ihr Teledat Router von jedem Rechner im Internet aus konfiguriert werden, vorausgesetzt das Passwort des Routers ist bekannt.

Bei deaktivierter Fernwartung kann ein externer Nutzer, welcher sich über ISDN, PPPoE oder IP-Routing in das lokale Netz eingewählt hat, den Router nicht konfigurieren.

Die Aktivierung der Option **Router ignoriert PING** verhindert, dass Ihr Teledat Router mittels **Ping** von außen gefunden werden kann.

Tipp

Ein **Ping** im Internet ist ein Datenpaket, welches an eine beliebige IP-Adresse gesendet werden kann. In der Regel wird dieses von der Gegenstelle beantwortet. Das Ping kann dazu missbraucht werden, potentielle Opfer für Hackerangriffe zu finden. Durch die oben gezeigte Einstellung verhindern Sie, dass Ihr Router auf solche Anfragen antwortet.

Über die Liste **Zugriff einschränken auf folgende IP-Adressen** können Sie den Zugriff auf Ihren Teledat Router weiter einschränken. Durch die Eingabe von **IP-Adresse** und **Teilnetzmaske** wird das Teilnetz definiert. Die Konfiguration des Routers aus dem Internet ist dann auf Rechner aus diesem Teilnetz beschränkt.

Tipp

Tragen Sie zum Beispiel die IP-Adresse 217.226.181.91 mit der zugehörigen Teilnetzmaske 255.255.255.255 ein, kann nur dieser Rechner den Router aus dem Internet konfigurieren. Um den Zugriff zu ermöglichen, muss zusätzlich die Fernwartung aktiviert sein.

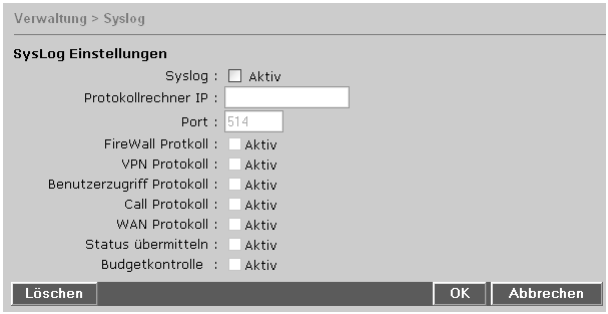
Im Bereich **Verwaltung über** legen Sie für **HTTP** einen Port fest, über den die Konfiguration erfolgen soll. Ab Werk ist für HTTP Port 80 eingestellt. Port 80 wird standardmässig verwendet, wenn Sie in Ihrem Webbrowser eine Internetadresse aufrufen.

Tipp

Wählen Sie einen anderen Port als 80, muss ein Nutzer diesen Port explizit angeben: Ihr Teledat Router hat zum Beispiel die öffentliche IP-Adresse 62.158.247.134 und 192.168.1.1 ist als LAN-Adresse vergeben. Der HTTP-Port für die Fernwartung ist mit 4500 eingestellt. Um den Konfigurator aufzurufen, ist im entfernten Rechner die Adresse 62.158.247.134:4500 im Browser einzugeben. Von einem Rechner im lokalen Netz aus ist der Konfigurator über die 192.168.1.1:4500 zu erreichen.

SysLog

Nutzen Sie die SysLog-Funktion, um Aktivitäten Ihres Teledat Routers an einen Protokollrechner zu übermitteln. Dazu gehören zum Beispiel Informationen zum Aufbau von Internetverbindungen oder die Abblockung von Anfragen durch die Firewall Ihres Routers.



Klicken Sie auf den Eintrag **Verwaltung** in der Menüleiste und wählen das Untermenü **SysLog**.

Damit **SysLog** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Tragen Sie im Feld **Protokollrechner IP** die IP-Adresse des Rechners ein, an den die Meldungen über die Aktivität des Routers verschickt werden sollen. Prüfen Sie ebenfalls den **Port**, über den die Nachrichten verschickt werden. Voreingestellt ist hier 514.

Auf der Konfigurationsseite sind alle die Meldungen aufgeführt, die über SysLog protokolliert werden können. Aktivieren Sie die für Sie relevanten Einträge, indem Sie bei dem jeweiligen Protokoll einen Haken vor **Aktiv** setzen. Möchten Sie zum Beispiel, dass Budgetinformationen protokolliert werden, ist es notwendig **Budgetkontrolle** zu aktivieren.

Bestätigen Sie Ihre Änderungen der SysLog-Einstellungen mit **OK**.

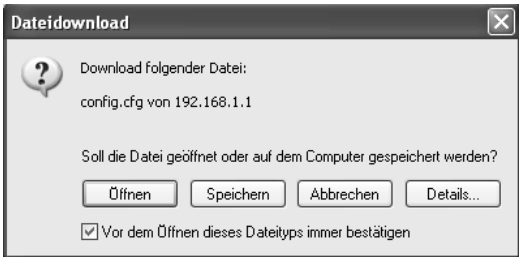
Am Protokollrechner können Sie zum Beispiel über das Utility **Teledat SysLog** die protokollierten Informationen abrufen. Eine Erläuterung dieses Tools finden Sie im Abschnitt **Routertools** (siehe Seite 82).

Konfig. sichern

Die Funktion **Konfiguration sichern** ermöglicht es Ihnen, die aktuellen Einstellungen Ihres Teledat Routers auf einem Rechner abzuspeichern. Sie können diese Konfiguration jederzeit wieder auf den Router laden.

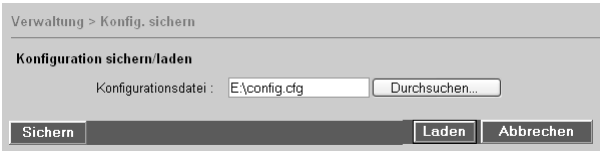
Klicken Sie auf den Eintrag **Verwaltung** in der Menüleiste und wählen das Untermenü **Konfig. sichern**.

Um die aktuellen Router-Einstellungen zu speichern, klicken Sie unten links auf **Sichern**.



Im folgenden Fenster klicken Sie auf **Speichern**, um die Datei mit dem Namen **config.cfg** zu sichern.

Wählen Sie im folgenden Fenster das Verzeichnis aus, in dem die Datei abgelegt werden soll.



Möchten Sie eine **Konfiguration laden**, geben Sie Verzeichnis und Namen der **Konfigurationsdatei** an und klicken auf **Laden**.

Beachten Sie, dass diese Funktion auch von Rechnern aus aufgerufen werden kann, die den Router über Fernwartung erreichen!

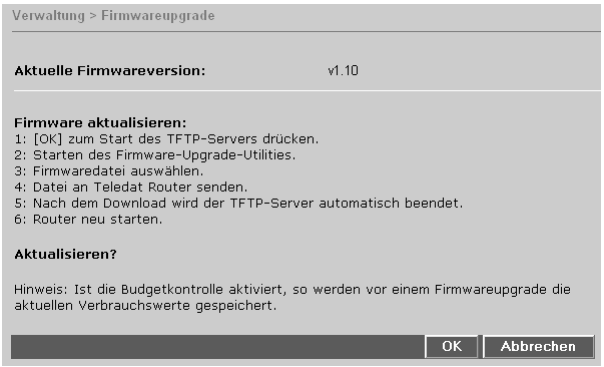
Firmwareupgrade

Die Firmware Ihres Teledat Routers ist vergleichbar mit dem Betriebssystem eines Computers und regelt dessen Funktionen. In diesem Abschnitt ist beschrieben, wie Sie die aktuelle Firmware Ihres Teledat Routers durch eine neuere Version ersetzen können. Aktuelle Firmware-Dateien finden Sie im Internet zum Download unter www.telekom.de/teledatrouter800.

Wir empfehlen Ihnen, unnötige Firmware-Upgrades zu vermeiden. Führen Sie Upgrades bitte nur dann durch, wenn die alte Version nicht korrekt funktioniert oder Sie eine neue Funktion des Updates benötigen! Die Dokumentation neuer Firmware-Versionen weist auf wichtige Neuerungen hin - bitte lesen Sie die Hinweise vor dem Upgrade!

Arbeiten Sie unter Windows, können Sie das Utility **Teledat Firmware Upgrade** einsetzen, welches Sie von der beigefügten CD installieren können. Eine genaue Beschreibung dieses Tools finden Sie auf Seite 83 in diesem Handbuch. In diesem Fall ist eine Vorbereitung des Teledat Routers auf das Upgrade nicht nötig.

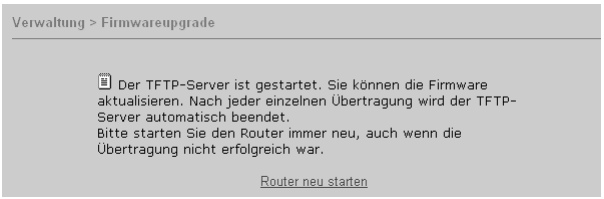
Alternativ können Sie ein beliebiges freies TFTP-Tool nutzen. Im Folgenden ist beschrieben, wie Sie eine neue Firmware (Datei *.all) mittels TFTP-Tool auf Ihren Teledat Router laden können.


Verwaltung > Firmwareupgrade
Aktuelle Firmwareversion: v1.10
Firmware aktualisieren:
1: [OK] zum Start des TFTP-Servers drücken.
2: Starten des Firmware-Upgrade-Utilities.
3: Firmwaredatei auswählen.
4: Datei an Teledat Router senden.
5: Nach dem Download wird der TFTP-Server automatisch beendet.
6: Router neu starten.
Aktualisieren?
Hinweis: Ist die Budgetkontrolle aktiviert, so werden vor einem Firmwareupgrade die aktuellen Verbrauchswerte gespeichert.
OK
Abbrechen

Klicken Sie auf den Eintrag **Verwaltung** in der Menüleiste und wählen das Untermenü **Firmwareupgrade**.

Hier ist die Schrittfolge für ein Firmware-Upgrade angegeben. Die aktuelle Firmwareversion ist oben rechts im Fenster angezeigt.

Klicken Sie auf **OK**.


Verwaltung > Firmwareupgrade
Der TFTP-Server ist gestartet. Sie können die Firmware aktualisieren. Nach jeder einzelnen Übertragung wird der TFTP-Server automatisch beendet.
Bitte starten Sie den Router immer neu, auch wenn die Übertragung nicht erfolgreich war.
Router neu starten

Das folgende Fenster informiert Sie darüber, dass der **TFTP-Server**, über den das Upgrade läuft, gestartet wurde.

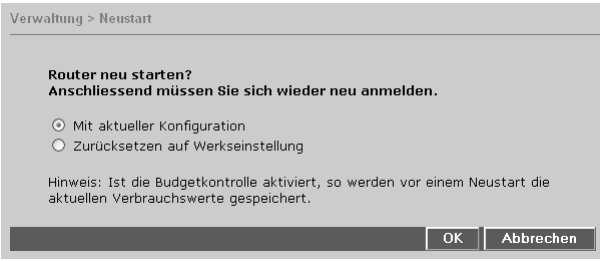
Öffnen Sie nun Ihr TFTP-Tool. Hier geben Sie in der Regel die IP Adresse Ihres Routers sowie Verzeichnis und Namen der Upgrade-Datei an. Anschließend wird die Datenübertragung gestartet. Ist diese beendet, erscheint eine Meldung über das erfolgreiche Upgrade auf Ihrem Bildschirm. Erhalten Sie stattdessen eine Fehlermeldung, starten Sie Ihren Teledat Router bitte neu und wiederholen das Upgrade.

Haben Sie die Upgrade-Datei erfolgreich geladen, starten Sie Ihren Teledat Router neu. Die neue Version der Firmware wird nun im Login-Fenster angezeigt.

Tipp

Sollten Sie Probleme mit dem Laden der Firmware haben, entfernen Sie den Netzstecker von Ihrem Teledat Router. Drücken Sie mit einem geeigneten Gegenstand (Stift) den Resetknopf direkt neben dem Netzanschluss. Schließen Sie nun den Netzstecker wieder an. Lassen Sie dabei den Resetknopf etwa drei Sekunden gedrückt. Nun springt der Router in den TFTP-Servermodus. Sie erkennen dies daran, dass die Diode **Power** schnell blinkt. Jetzt können Sie die Firmware direkt über das TFTP-Tool auf den Router laden. Ein Zugriff auf den Router über den Web-Konfigurator ist in diesem Fall nicht erforderlich.

Neustart


Verwaltung > Neustart
Router neu starten?
Anschliessend müssen Sie sich wieder neu anmelden.
Mit aktueller Konfiguration
Zurücksetzen auf Werkseinstellung
Hinweis: Ist die Budgetkontrolle aktiviert, so werden vor einem Neustart die aktuellen Verbrauchswerte gespeichert.
OK
Abbrechen

Klicken Sie in der Menüleiste auf den Eintrag **Verwaltung** und wählen das Untermenü **Neustart**.

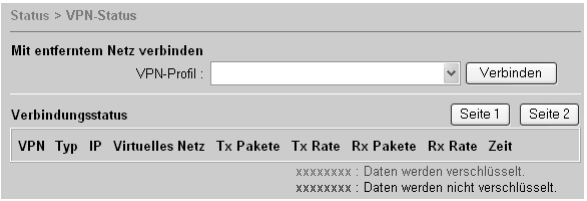
Klicken Sie auf **OK**, um den Router mit der aktuellen Konfiguration neu zu starten.

Möchten Sie den Router auf die Werkseinstellungen zurücksetzen, aktivieren Sie bitte die Einstellung **Zurücksetzen auf Werkseinstellung** und klicken Sie anschließend auf **OK**.

Status

Ihr Teledat Router stellt Ihnen eine Reihe von Menüs zur Verfügung, die seinen aktuellen Zustand anzeigen.

VPN Status


Status > VPN-Status
Mit entferntem Netz verbinden
VPN-Profil :
Verbinden
Verbindungsstatus
Seite 1
Seite 2
VPN Typ IP Virtuelles Netz Tx Pakete Tx Rate Rx Pakete Rx Rate Zeit
xxxxxxxx : Daten werden verschlüsselt.
xxxxxxxx : Daten werden nicht verschlüsselt.

Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **VPN Status**, um Informationen über bestehende VPN-Verbindungen abzurufen.

Sie können in diesem Menü auch VPN oder LAN-LAN Verbindungen manuell aufbauen oder beenden. Wählen Sie dazu ein **VPN-Profil** aus der Liste im Bereich **Mit entferntem Netz verbinden** und klicken Sie auf **Verbinden**.

Ist eine Verbindung erstellt, werden unter **Verbindungsstatus** die aktuellen Daten angezeigt.

Sind die Einträge grün dargestellt, weist das auf eine verschlüsselte Verbindung hin. Schwarze Einträge zeigen an, dass keine Verschlüsselung vorgenommen wurde.

Unter **VPN** erscheint die Nummer der aktuellen Verbindung sowie der Name des LAN-LAN-Profils.

Mit **Typ** wird die Art der Netzwerkverbindung, das heisst Übertragungsprotokoll und Verschlüsselung angegeben.

Der nächsten Spalte können Sie die **WAN-IP-Adresse** des entfernten Routers entnehmen.

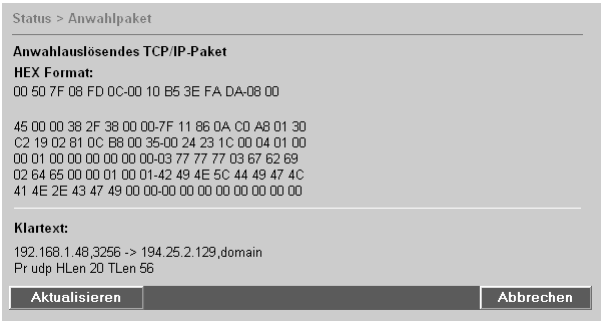
Unter **Virtuelles Netz** finden Sie die Angabe zum Adressraum des entfernten Netzwerks.

Die Einträge unter **TX Pakete** beziehungsweise **RX Pakete** geben an, wieviele Datenpakete versandt (TX) und empfangen (RX) wurden. Mit **TX Rate** beziehungsweise **RX Rate** wird die jeweilige Übertragungsgeschwindigkeit angegeben.

Die **Zeit** gibt an, wie lange die Verbindung bereits aktiv ist.

Klicken Sie auf **Trennen**, um eine bestehende Verbindung zu beenden.

Anwahlpaket



Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **Anwahlpaket**, um Informationen über die Ursache der Einwahl in das Internet abzurufen.

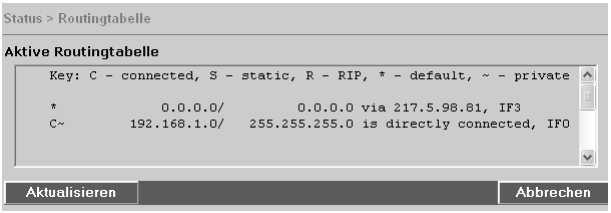
Der Bereich **Klartext** enthält Angaben zu dem Datenpaket, das die Einwahl ins Internet ausgelöst hat. Sie können der ersten Zeile die IP-Adresse des auslösenden Rechners entnehmen. Weiterhin sind Informationen zur Art der Anfrage aufgeführt.

In obigem Beispiel wird die Internetanwahl durch den Rechner mit der IP-Adresse 192.168.1.48 über den Port 3256 ausgelöst. Der Rechner schickt eine Anfrage an die IP-Adresse 194.25.2.129. Die Angabe **domain** bedeutet, dass es sich hier um einen Domain Name Server handelt (der DNS von T-Online), welcher eine im Web-Browser eingegebene Adresse in die richtige IP-Adresse umwandeln soll.

Tipp

Rufen Sie diesen Menüpunkt zum Beispiel dann auf, wenn Ihnen unklar ist, warum eine Einwahl ins Internet ausgelöst wurde.

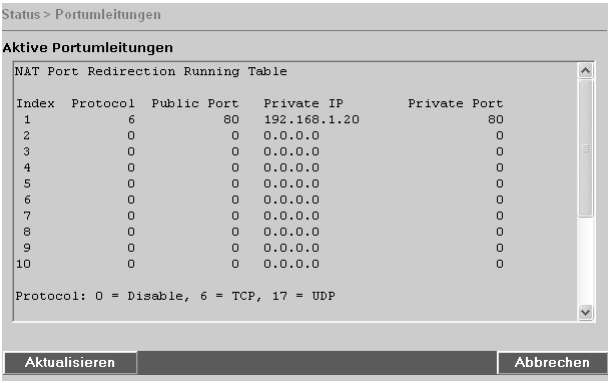
Routingtabelle


Status > Routingtabelle
Aktive Routingtabelle
Key: C - connected, S - static, R - RIP, * - default, ~ - private
* 0.0.0.0/ 0.0.0.0 via 217.5.98.81, IF3
C~ 192.168.1.0/ 255.255.255.0 is directly connected, IF0
Aktualisieren
Abbrechen

Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **Routingtabelle**, um die aktuelle Routingtabelle anzuzeigen.

Dieser Tabelle können Sie Angaben zu den Netzwerken entnehmen, mit welchen Ihr Router derzeit verbunden ist.

Portumleitungen


Status > Portumleitungen
Aktive Portumleitungen
NAT Port Redirection Running Table
Index Protocol Public Port Private IP Private Port
1 6 80 192.168.1.20 80
2 0 0 0.0.0.0 0
3 0 0 0.0.0.0 0
4 0 0 0.0.0.0 0
5 0 0 0.0.0.0 0
6 0 0 0.0.0.0 0
7 0 0 0.0.0.0 0
8 0 0 0.0.0.0 0
9 0 0 0.0.0.0 0
10 0 0 0.0.0.0 0
Protocol: 0 = Disable, 6 = TCP, 17 = UDP
Aktualisieren
Abbrechen

Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **Portumleitungen**.

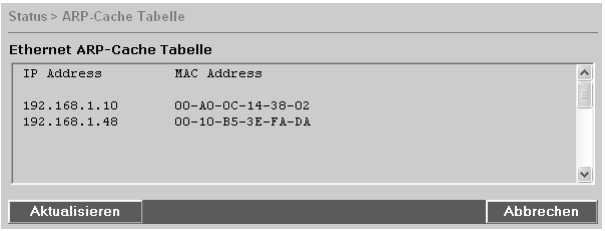
Hier sind die aktuellen Portumleitungen aufgeführt.

Die Einträge sind unter **Index** laufend nummeriert.

Anhand der Angabe unter **Protocol** können Sie erkennen, ob die Portumleitung für **TCP/IP**- (6) oder **UDP** (7)-Verbindungen gültig ist. Ist eine 0 eingetragen, so ist der Eintrag nicht aktiv.

Public Port gibt den Öffentliche Port an, dessen Daten an die **Private IP** (IP-Adresse im lokalen Netzwerk) über den **Private Port** (Port im lokalen Netzwerk) weitergeleitet werden sollen.

ARP Cache

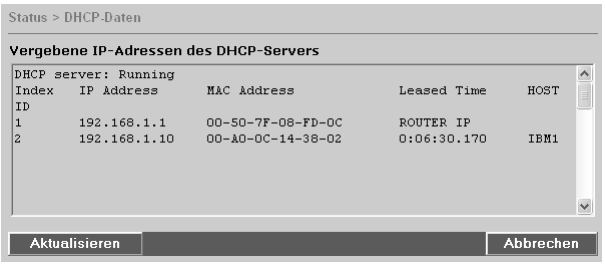


Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **ARP Cache.**

Hier wird die aktuellen ARP Tabelle angezeigt.

In der ARP Tabelle sind die IP- und Hardware (MAC) - Adressen aller Rechner aufgeführt, die mit dem Router im lokalen Netz verbunden sind.

DHCP Daten



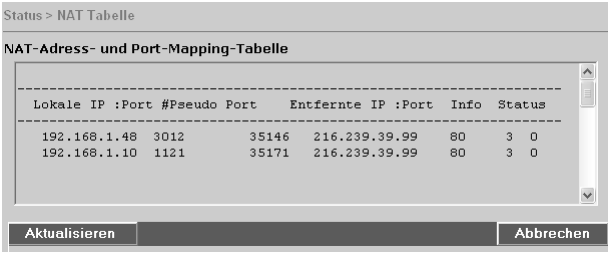
Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **DHCP Daten**.

Hier wird die aktuelle DHCP-Tabelle angezeigt.

Der erste Index zeigt die Angaben Ihres Teledat Routers. Neben der IP-Adresse (zum Beispiel 192.168.1.1) ist die MAC-Adresse aufgeführt sowie der Hinweis, dass es sich um die feste IP-Adresse (FIXED IP) handelt.

Ab der zweiten Zeile sind die DHCP-Clients aufgeführt. Es werden jeweils die IP-Adresse, MAC-Adresse und Verbindungszeit angegeben.

NAT Adresstabelle


Status > NAT Tabelle
NAT-Adress- und Port-Mapping-Tabelle
Lokale IP :Port #Pseudo Port Entfernte IP :Port Info Status
192.168.1.48 3012 35146 216.239.39.99 80 3 0
192.168.1.10 1121 35171 216.239.39.99 80 3 0
Aktualisieren
Abbrechen

Klicken Sie in der Menüleiste auf den Eintrag **Status** und wählen das Untermenü **NAT Adresstabelle**, um Informationen über die aktuellen Adress- und Port-Zuweisungen zu erhalten.

Für jede Anfrage werden die **Lokale IP-Adresse** und **Port** des anfragenden Rechners angegeben. Weiterhin können Sie dieser Tabelle **Entfernte IP** und **Port** der angefragten Internetseite entnehmen.

Anwendungen mit dem Teledat Router 800

In diesem Kapitel werden Beispiele für die Konfiguration Ihres Teledat Routers aufgezeigt.

LAN-LAN-Kopplung mit VPN über Internet

Über VPN können Sie zwei lokale Netzwerke über das Internet miteinander verbinden. Die Verbindung kann mittels IPSec gesichert werden. Um eine VPN-Verbindung aufzubauen, benötigen Sie zwei Router, die über bekannte IP-Adressen mit dem Internet verbunden sind. In den folgenden Beispielen werden zwei Teledat Router 800 eingesetzt. Der erste Router befindet sich in der **Zentrale** und besitzt die IP-Adresse **192.168.1.1**, während sich der zweite Teledat Router mit der IP-Adresse **192.168.5.1** in der **Außenstelle** befindet.

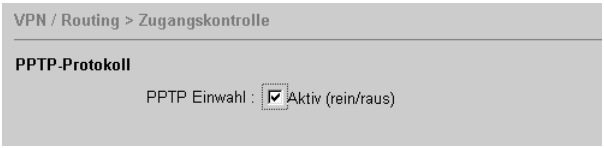
Unidirektionale LAN-LAN-Kopplung

Unidirektionale Kopplung heisst, es wird eine einseitige Verbindung aufgebaut. Der Datentransfer erfolgt nur in eine Richtung. Nur der Anrufer kann Daten anfordern und senden.

Diese Art des Verbindungsaufbaus empfehlen wir, wenn Sie zum Beispiel vom Heimbüro aus auf zentrale Daten in der Firma zugreifen möchten oder wenn Sie eine Fernwartung Ihres Rechners zum Beispiel über Timbuktu oder PC-Anywhere durchführen möchten.

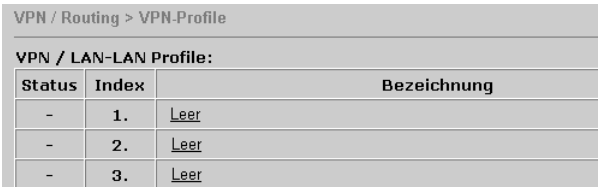
Im nachfolgenden Beispiel wird der Verbindungsaufbau anhand einer PPTP-Verbindung erklärt. Der Router in der **Außenstelle** soll auf das Netzwek in der **Zentrale** zugreifen können. Umgekehrt soll kein Zugriff möglich sein. Beide Router müssen für das VPN Netzwerk konfiguriert werden.

Konfigurieren Sie zunächst den Router in der **Zentrale**.



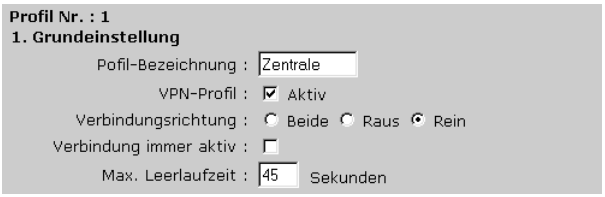
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Zugangskontrolle**.

Aktivieren Sie hier die Protokolle, die für die VPN-Verbindug benutzt werden sollen. Für unser Beispiel aktivieren Sie den Eintrag **PPTP Einwahl**.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **VPN Profile**.

Klicken Sie auf ein freies Profil für Ihre VPN-Verbindung, im Beispiel auf **Leer** neben dem **Index 1.**

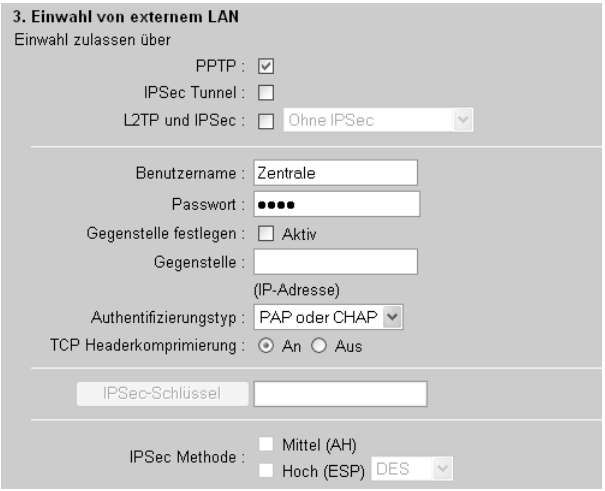


Im Bereich **Grundeinstellung** vergeben Sie zunächst eine **Profil-Bezeichnung**, zum Beispiel **Zentrale**.

Damit das **VPN-Profil** wirksam wird, setzen Sie einen Haken neben **Aktiv**.

Der Aufbau des VPN-Netzes soll nur vom entfernten Router aus möglich sein. Klicken Sie deshalb bei **Verbindungsrichtung** auf **Rein**.

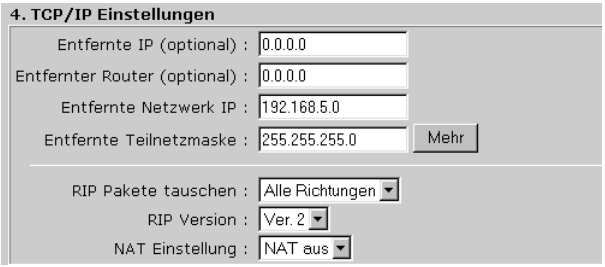
Eintragungen im zweiten Bereich **Verbindungsaufbau zu externem LAN** entfallen, da die Verbindung nur in einer Richtung aufgebaut werden soll.



Im dritten Abschnitt **Einwahl von externem LAN** aktivieren Sie im Bereich **Einwahl zulassen über** den Eintrag **PPTP**.

Tragen Sie **Benutzername** und **Passwort** für diese VPN-Verbindung ein. Im Beispiel wird der Benutzername **Zentrale** und das Passwort **1234** verwendet.

Gegenstelle festlegen wird nicht aktiviert.



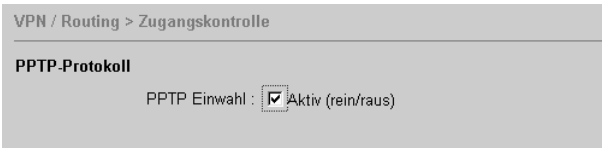
Nehmen Sie jetzt die **TCP/IP-Einstellungen** vor.

Für unser Beispiel ist es ausreichend, die **Entfernte Netzwerk IP** und die **Entfernte Teilnetzmaske** anzugeben.

Im Beispiel ist die **Entfernte Netzwerk IP** mit 192.168.5.0 und die **Entfernte Teilnetzmaske** mit 255.255.255.0 angegeben. Wählen Sie bei **RIP Pakete tauschen** den Eintrag **Alle Richtungen** und bei **RIP Version** den Eintrag **Ver.2**. Achten Sie darauf, dass Sie als **NAT Einstellung** für die Zentrale **NAT aus** angeben. Damit ermöglichen Sie von der Außenstelle aus den Zugriff auf die Rechner der Zentrale.

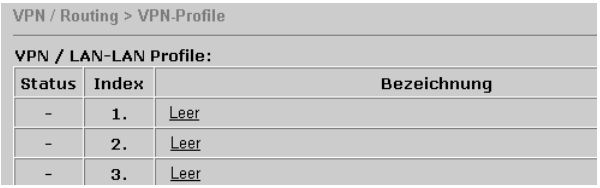
Die Konfiguration des Routers in der Zentrale ist jetzt abgeschlossen. Bestätigen Sie Ihre Eingaben mit **OK**.

Konfigurieren Sie im zweiten Schritt den Router Ihrer **Außenstelle**.



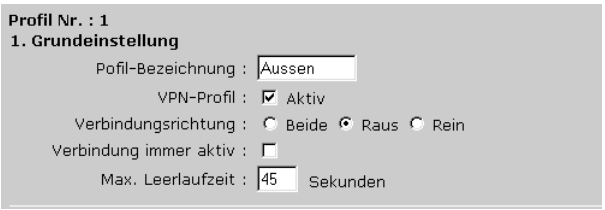
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Zugangskontrolle**.

Aktivieren Sie hier für unser Beispiel den Eintrag **PPTP Einwahl**.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **VPN Profile**.

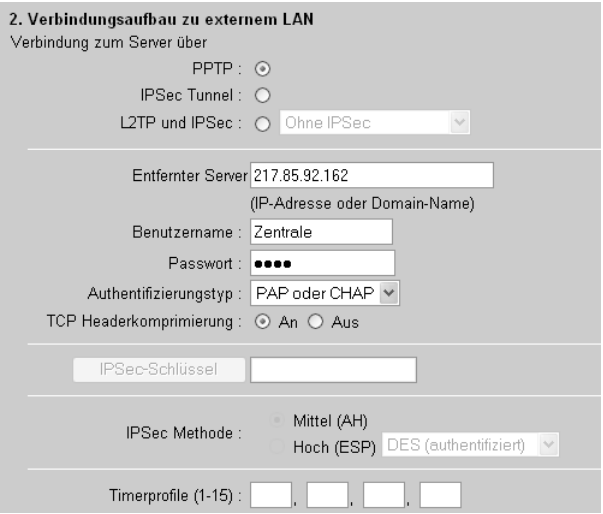
Klicken Sie auf ein freies Profil für Ihre VPN-Verbindung, im Beispiel auf **Leer** neben dem **Index 1.**



Im Bereich **Grundeinstellung** vergeben Sie zunächst eine **Profil-Bezeichnung**, zum Beispiel **Aussen**.

Damit das **VPN-Profil** wirksam wird, setzen Sie einen Haken neben **Aktiv**.

Der Aufbau des VPN-Netzes soll nur von diesem Router aus möglich sein. Klicken Sie deshalb bei **Verbindungsrichtung** auf **Raus**.



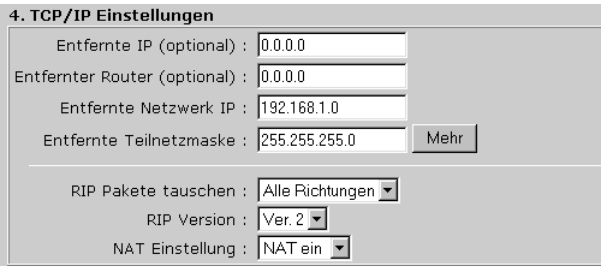
Im zweiten Abschnitt **Verbindungsaufbau zu externem LAN** aktivieren Sie bitte im Bereich **Verbindung zum Server über** den Eintrag **PPTP**.

Im Feld **Entfertner Server** geben Sie die WAN IP-Adresse des Routers der Zentrale ein, im Beispiel die 217.85.92.162.

Tragen Sie bei **Benutzername** den Namen ein, den Sie im Router der Zentrale als **Benutzernamen** vergeben haben.

Im Beispiel ist das **Zentrale**. Als **Passwort** geben Sie bitte auch das Passwort ein, das Sie bei der Zentrale eingegeben haben, im Beispiel **1234**.

Für diesen Teledat Router in der Außenstelle ist der Abschnitt **3. Verbindungsaufbau von externem LAN** nicht relevant.

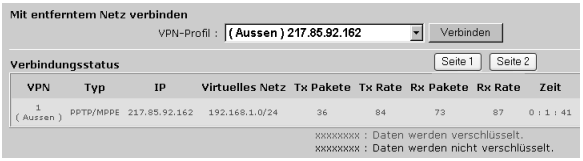


Tragen Sie bei **TCP/IP-Einstellungen** die 192.168.1.0 als **Entfernte Netzwerk IP** und 255.255.255.0 als **Entfernte Teilnetzmaske** des Netzes der Zentrale ein.

Wählen Sie bei **RIP Pakete tauschen** den Eintrag **Alle Richtungen** und bei **RIP Version** den Eintrag **Ver. 2**. Die **NAT Einstellung** legen Sie bitte mit **NAT ein** fest. Damit verhindern Sie, dass Rechner im Netzwerk der Zentrale während der VPN-Verbindung auf den oder die Rechner der Außenstelle zugreifen können.

Nun ist Ihr Router der Außenstelle ebenfalls konfiguriert. Bestätigen Sie Ihre Eingaben mit **OK**.

Jetzt können Sie Ihre unidirektionale VPN-Verbindung vom Router der **Außenstelle** aus testen. Öffnen Sie hierfür im Bereich **Status** das Menü **VPN Status.** Wählen Sie das **VPN-Profil** aus der Liste im Bereich **Mit entferntem Netz verbinden** und klicken Sie auf **Verbinden**.



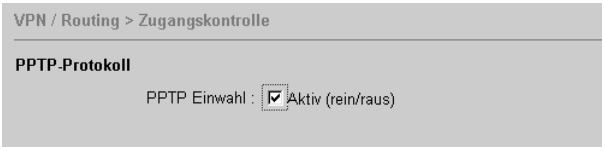
Ist die Verbindung erstellt, werden unter **Verbindungsstatus** die aktuellen Daten der Verbindung angezeigt.

Bidirektionale LAN-LAN-Kopplung

Bei einer **bidirektionalen** VPN-Verbindung kann die Verbindung von beiden Netzwerken aus aufgebaut werden. Rechner aus beiden Netzwerken können Adressen im jeweils anderen Netzwerk erreichen.

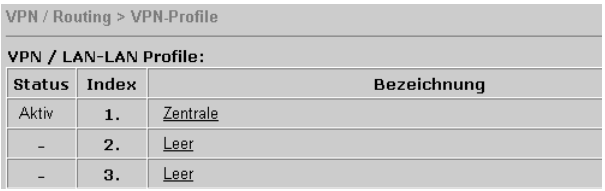
Im nachfolgenden Beispiel wird der Aufbau anhand einer PPTP-Verbindung erklärt. Das Netzwerk einer **Außenstelle** soll mit dem Netzwek der **Zentrale** verbunden werden. Der Zugriff soll in beiden Richtungen möglich sein. Beide Router müssen für das VPN-Netzwerk konfiguriert werden. Die Einstellungen stimmen bei beiden Routern weitgehend überein. Auf Abweichungen wird hingewiesen.

Definieren Sie im ersten Schritt die Protokolle, die für die VPN-Verbindung benutzt werden sollen.



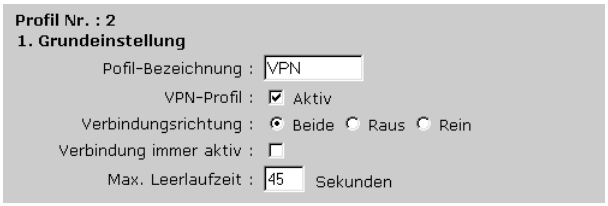
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Zugangskontrolle**.

Aktivieren Sie den Eintrag **PPTP Einwahl**. Definieren Sie nun das Profil für Ihre VPN-Verbindung.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **VPN Profile**.

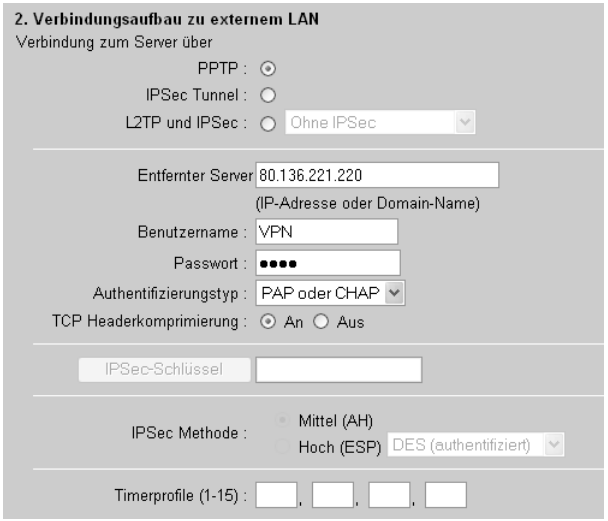
Klicken Sie auf ein freies Profil für Ihre VPN-Verbindung, im Beispiel auf **Leer** neben **Index 2**.



Im Bereich **Grundeinstellung** vergeben Sie zunächst eine **Profil-Bezeichnung**, zum Beispiel **VPN**.

Damit das **VPN-Profil** wirksam wird, setzen Sie einen Haken neben **Aktiv**.

Der Aufbau des VPN-Netzes soll von beiden Netzen aus möglich sein. Klicken Sie deshalb bei **Verbindungsrichtung** auf **Beide**.



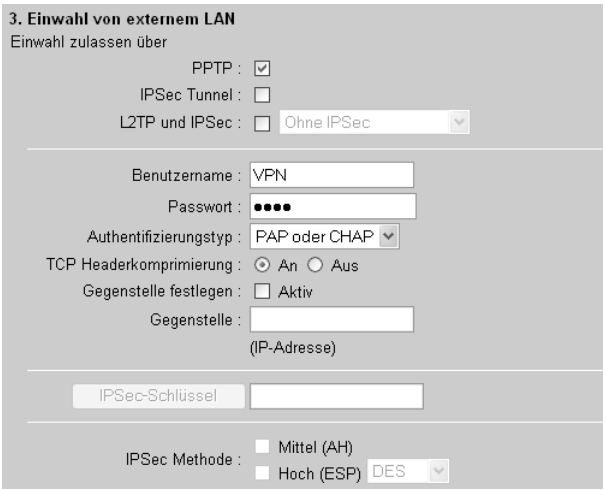
Definieren Sie jetzt die Eigenschaften für den **Verbindungsaufbau zu externem LAN**.

Als Protokoll für die Einwahl bei dem anderen Router wählen Sie **PPTP**.

Geben Sie als **Entfernter Server** bitte jeweils die WAN-IP-Adresse des Routers der Gegenstelle an. Das bedeutet, dieser Eintrag muss bei beiden Routern **unterschiedlich** sein.

Im Teledat Router der Zentrale tragen Sie bitte die IP-Adresse der Außenstelle ein, im Beispiel die 80.136.221.220. Dagegen wird als **Entfernter Server** bei der Außenstelle die IP-Adresse des Routers der Zentrale mit 217.85.92.162 angegeben.

Im Beispiel wird der Benutzername **VPN** und das Passwort **1234** bei beiden Routern als Kennung für den Verbindungsaufbau zu externem LAN verwendet.

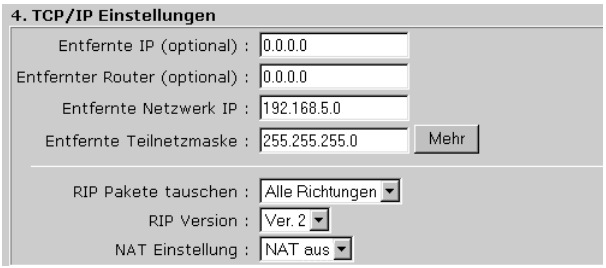


Im Bereich **Einwahl von externem LAN** aktivieren Sie bei **Einwahl zulassen über** den Eintrag **PPTP**.

Tragen Sie **Benutzername** und **Passwort** analog den Angaben bei der Gegenstelle unter **Verbindungsaufbau zu externem LAN** ein. Im Beispiel ist das der Benutzername **VPN** und das Passwort **1234**.

Tipp

Achten Sie darauf, dass Benutzerkennung und Passwort im Bereich **Einwahl von externem LAN** mit den Angaben übereinstimmen, die Sie bei der jeweiligen Gegenstelle unter **Verbindungsaufbau zum externen LAN** festgelegt haben.



Tragen Sie bei **TCP/IP-Einstellungen** jeweils die **Entfernte Netzwerk IP** und die **Entfernte Teilnetzmaske** des Netzes der Gegenstelle ein.

Bei der Beispielkonfiguration wird bei der Zentrale die **192.168.5.0** und bei der Außenstelle die **192.168.1.0** als **Entfernte Netzwerk IP** eingetragen. Die **Entfernte Teilnetzmaske** ist bei beiden Profilen mit **255.255.255.0** angegeben.

Prüfen Sie in jedem Fall die **NAT Einstellung**. Bei beiden Routern muss **NAT aus** aktiviert sein, damit die Verbindung in beiden Richtungen nutzbar ist.

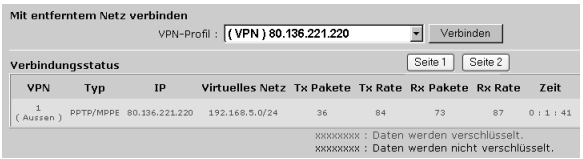
Tipp

Netzwerke mit gleichen IP-Adressen können nicht verbunden werden!

Haben Sie mehrere Verbindungen zu verschiedenen Netzen definiert, wird ein bestimmtes Netzwerk automatisch angewählt, sobald eine Adresse dieses entfernten Netzwerks angefragt wird. Das funktioniert aber nur, wenn die entfernten Netze unterschiedliche **Entfernte Netzwerk IPs** haben. Ist das nicht der Fall, wird das erste aktive Profil in der Profil-Liste (siehe VPN /LAN-LAN Verbindungen) angewählt, welches die passende Entfernte Netzwerk IP besitzt. Um das gewünschte Profil festzulegen, deaktivieren Sie alle anderen Profile mit der gleichen Entfernten Netzwerk IP.

Bestätigen Sie Ihre Änderungen zum Profil jeweils mit **OK**.

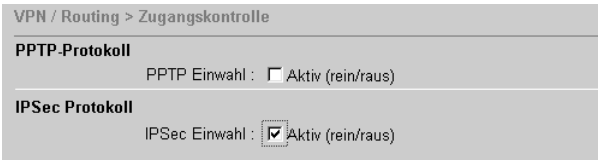
Jetzt können Sie Ihre VPN-Verbindung von beiden Routern aus testen. Öffnen Sie hierfür im Bereich **Status** jeweils das Menü **VPN Status.** Wählen Sie das **VPN-Profil** aus der Liste im Bereich **Mit entferntem Netz verbinden** und klicken Sie auf **Verbinden**.


Mit entferntem Netz verbinden
VPN-Profil : (VPN) 80.136.221.220
Verbinden
Verbindungsstatus
Seite 1
Seite 2
VPN Typ IP Virtuelles Netz Tx Pakete Tx Rate Rx Pakete Rx Rate Zeit
1 (Aussen) PPTP/MPPE 80.136.221.220 192.168.5.0/24 36 84 73 87 0 : 1 : 41
xxxxxxxx : Daten werden verschlüsselt.
xxxxxxxx : Daten werden nicht verschlüsselt.

Ist die Verbindung erstellt, werden unter **Verbindungsstatus** die aktuellen Daten der Verbindung angezeigt.

Bidirektionale LAN-LAN-Kopplung mit IPSec Verschlüsselung

Ihr Teledat Router bietet Ihnen die Möglichkeit, VPN-Verbindungen über einen IPSec-Tunnel aufzubauen. Im Beispiel wird ein solcher Tunnel zwischen zwei Teledat Routern 800 aufgebaut. Beide Router müssen hierfür konfiguriert werden.

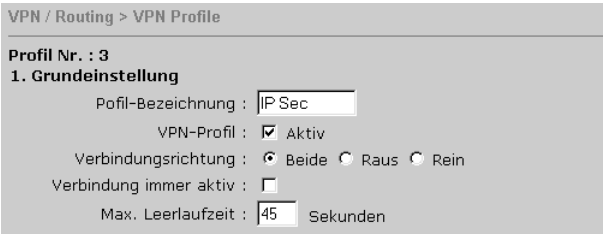


Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Zugangskontrolle**.

Aktivieren Sie hier die Option **IPSec Einwahl**.

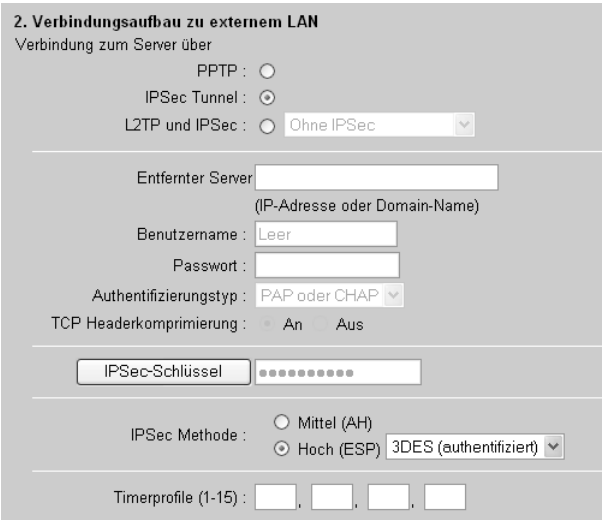
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **VPN Profile**.

Klicken Sie auf ein freies Profil für Ihre VPN-Verbindung, im Beispiel auf **Leer** neben **Index 3.**



Im Bereich **Grundeinstellung** vergeben Sie zunächst eine **Profil-Bezeichnung**, zum Beispiel **IPSec**.

Aktivieren Sie das **VPN Profil**. Als Verbindungsrichtung wählen Sie **Beide**.



Im zweiten Abschnitt **Verbindungsaufbau zu externem LAN** aktivieren Sie jetzt **IPSec Tunnel**.

Tragen Sie die **IP-Adresse** des jeweils **Entfernten Servers** ein. Im Teledat Router der Zentrale tragen Sie bitte die IP-Adresse der Außenstelle ein, im Beispiel die 80.136.221.220.

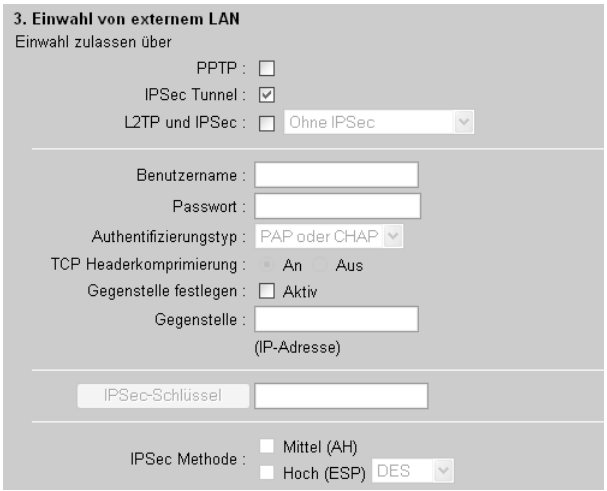
Dagegen wird bei der Außenstelle als **Entfernter Server** die IP-Adresse des Routers der Zentrale mit 217.85.92.162 angegeben.

Bei IPSec erfolgt die Authentifizierung über einen Schlüssel; somit entfällt die Eingabe von Benutzername und Passwort.

Klicken Sie auf den Button **IPSec-Schlüssel**, um den Schlüssel für die Anwahl des entfernten Routers anzugeben.

Geben Sie hier jeweils den **IPSec-Schlüssel** an, den Sie bei der Gegenstelle als Schlüssel für die Einwahl in den Router festgelegt haben. Bestätigen Sie die Eingabe im Feld **IPSec-Schlüssel bestätigen**.

Legen Sie im nächsten Schritt fest, auf welchem IPSec-Sicherheitsniveau die Anwahl des entfernten Routers erfolgen soll. Im Beispiel ist bei beiden Routern als **IPSec Methode** die Option **Hohe Sicherheit (ESP)** mit **3DES** eingestellt. Mit dieser Einstellung erfolgt eine dreifache Verschlüsselung der zu übertragenden Daten.



Im dritten Bereich **Einwahl von externem LAN** beschränken sich die Einstellungen unter **Einwahl zulassen über** auf die Auswahl der Option **IPSec Tunnel**.

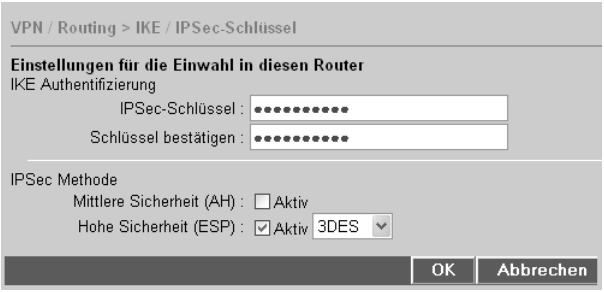
Die Option **Gegenstelle festlegen** wird nicht aktiviert. Ein profilspezifischer IPSec-Schlüssel kann damit nicht angegeben werden; für die Einwahl in den Router ist der unter **VPN/Routing–> IKE/IPSec-Schlüssel** festgelegte Schlüssel gültig.

Die **TCP/IP Einstellungen** im vierten Bereich nehmen Sie analog dem vorhergehenden Beispiel vor. Bei der Zentrale wird die **192.168.5.0** und bei der Außenstelle die **192.168.1.0** als **Entfernte Netzwerk IP** eingetragen. Die **Entfernte Teilnetzmaske** ist bei beiden Profilen mit **255.255.255.0** angegeben.

Prüfen Sie in jedem Fall die **NAT Einstellung**. Bei beiden Routern muss **NAT aus** aktiviert sein, damit die Verbindung in beiden Richtungen nutzbar ist.

Klicken Sie zum Speichern Ihrer Einstellungen auf **OK**.

Nehmen Sie im zweiten Schritt die Definition Ihres IPSec-Schlüssels für die Einwahl vor. Es ist bei beiden Routern ein Schlüssel für die Einwahl in den Router anzugeben.



Öffnen Sie in der Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **IKE/IPSec-Schlüssel**.

Tragen Sie im Bereich **Einstellungen für die Einwahl in diesen Router** unter **IKE Authentifizierung** den **IPSec-Schlüssel** ein (im Beispiel 0123456789), der bei der Einwahl in den Router der Zentrale eingesetzt werden soll. Wiederholen Sie Ihre Eingabe bei **IPSec-Schlüssel bestätigen**. Ihr Teledat Router überprüft, ob die beiden Einträge übereinstimmen. Achten Sie darauf, dass bei der Außenstelle dieser Schlüssel als **Schlüssel für die Anwahl des anderen Routers** angegeben werden muss.

Legen Sie im nächsten Schritt fest, auf welchem IPSec-Sicherheitsniveau die Einwahl erfolgen kann.
Im Beispiel ist als **IPSec Methode** die Option **Hohe Sicherheit (ESP)** mit **3DES** eingestellt. Mit dieser Einstellung erfolgt eine dreifache Verschlüsselung der zu übertragenden Daten.

Damit ist der Router der Zentrale für die **Einwahl** durch den Router der Außenstelle über IPSec Tunnel konfiguriert.

Nehmen Sie nun analog die Einstellungen für die Einwahl durch die Gegenstelle beim Router der Aussenstelle vor.

Beachten Sie, dass Sie als Schlüssel für die Anwahl des anderen Routers jeweils den gleichen Schlüssel angeben, der bei der Gegenstelle als Schlüssel für die Einwahl in diesen Router angegeben wurde.

Sind beide Schlüssel bei beiden Routern angegeben, können Sie den Aufbau Ihres IPSec-Tunnels von einem der Router aus testen. Öffnen Sie hierfür im Bereich **Status** jeweils das Menü **VPN Status.** Wählen Sie das **VPN-Profil** aus der Liste im Bereich **Mit entferntem Netz verbinden** und klicken Sie auf **Verbinden.**

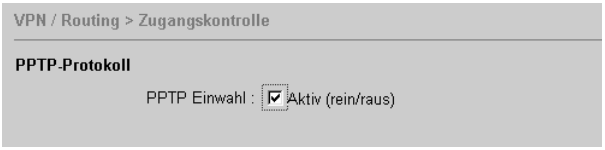
Ist die Verbindung erstellt, werden unter **Verbindungsstatus** die aktuellen Daten der Verbindung angezeigt.

Entfernte Nutzer einbinden

Nutzerprofil definieren

Dieses Beispiel zeigt, wie Sie Ihren Teledat Router für die Einwahl durch entfernte Nutzer konfigurieren können. Die Verbindung wird über das Internet erstellt.

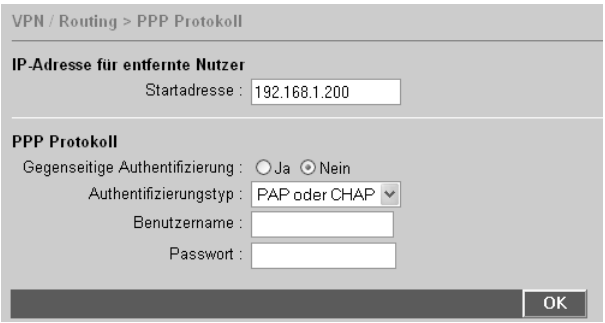
Legen Sie im ersten Schritt fest, welche Protokolle für die Verbindung verwendet werden sollen.



Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **Zugangskontrolle**.

Aktivieren Sie den Eintrag **PPTP** und klicken Sie auf **OK**.

Im zweiten Schritt nehmen Sie die Konfiguration der Verbindung vor.



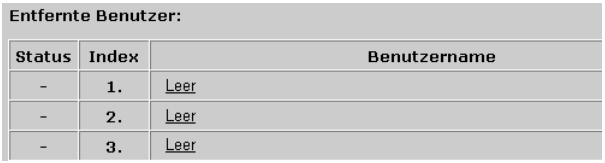
Klicken Sie in der Menüleiste Ihres Teledat Routers auf **VPN/Routing** und wählen Sie aus dem angezeigten Untermenü den Eintrag **PPP Protokoll**.

Prüfen Sie hier die **Startadresse** für die entfernten Nutzer.

Die **Startadresse** ist die IP-Adresse, die an den ersten entfernten Nutzer der sich einwählt, vergeben wird. Übernehmen Sie hier die voreingestellte Adresse 192.168.1.200. Ein weiterer entfernter Nutzer erhält die auf diese Startadresse folgende IP-Adresse (im Beispiel also 192.168.1.201). Achten Sie darauf, dass die zu vergebenden Adressen nicht im Adressbereich des DHCP-Servers liegen. Bitte vergewissern Sie sich, dass die IP-Adresse noch nicht in Ihrem Netz vergeben ist und freigehalten wird.

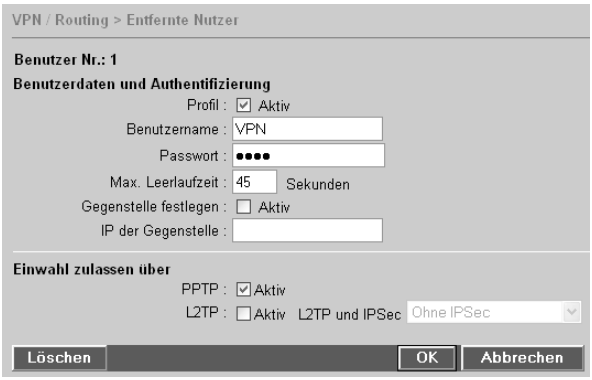
Die **Gegenseitige Authentifizierung** können Sie bei der Voreinstellung **Nein** belassen. Dann bleiben die Einträge für **Benutzername** und **Passwort** frei; sie sind nur erforderlich, wenn gegenseitige Authentifizierung genutzt wird. Speichern Sie Änderungen bitte mit **OK**.

Definieren Sie anschliessend das Nutzerprofil.



Öffnen Sie in Ihrer Menüleiste den Bereich **VPN/Routing** und wählen aus dem Untermenü den Eintrag **Entfernte Nutzer**.

Klicken Sie auf ein freies Nutzerprofil im Beispiel auf **Leer** neben **Index 1**.



Damit das **Profil** wirksam wird, setzen Sie einen Haken vor **Aktiv**.

Tragen Sie jetzt als **Benutzername** zum Beispiel **VPN** und das **Passwort** mit **1234** in den zugehörigen Feldern ein.

Mit diesen Daten muss sich der entfernte Nutzer bei der Einwahl identifizieren.

Die Option **Gegenstelle festlegen** wird im Beispiel nicht aktiviert.

Die Kombination von Benutzername und Kennwort muss eindeutig sein. Das heisst, für ein weiteres Profil darf eine einmal vergebene Kombination nicht nochmals vergeben werden.

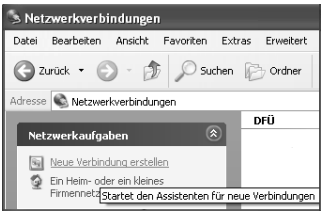
Unter **Einwahl zulassen über** muss die Option **PPTP** aktiviert sein. Damit legen Sie fest, dass die Einwahl über das Protokoll PPTP zugelassen wird. Die anderen Optionen können Sie für das Beispiel deaktivieren.

Klicken Sie auf **OK**, um die Einstellungen zu speichern. Der entfernte Nutzer kann sich nun einwählen.

Im Bereich **Status** unter **VPN Status** werden die aktuellen Daten der Verbindung angezeigt.

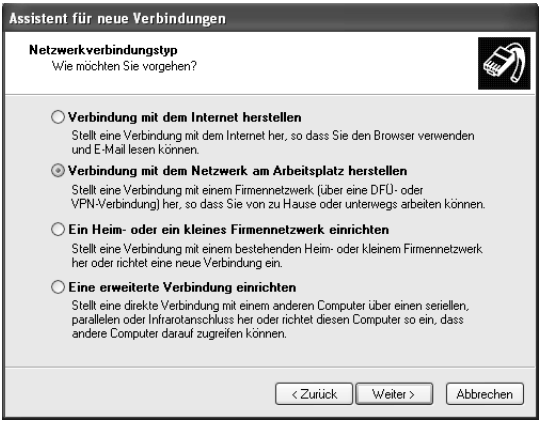
Benutzereinwahl über Windows XP

Im Folgenden wird gezeigt, wie Sie unter Windows XP einen PC für die Einwahl via PPTP-Protokoll in Ihren Teledat Router konfigurieren können. Öffnen Sie zunächst das **Startmenü**. Klicken Sie auf **Systemsteuerung** und wählen hier **Netzwerk- und Internetverbindungen**.



Um eine neue Verbindung zu erstellen, klicken Sie auf **Neue Verbindung erstellen**.

Der **Assistent für neue Verbindungen** wird geöffnet. Klicken Sie im ersten Fenster des Assistenten auf **Weiter**.


Assistent für neue Verbindungen
Netzwerkverbindungstyp
Wie möchten Sie vorgehen?
Verbindung mit dem Internet herstellen
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
Verbindung mit dem Netzwerk am Arbeitsplatz herstellen
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFÜ- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
Ein Heim- oder ein kleines Firmennetzwerk einrichten
Stellt eine Verbindung mit einem bestehenden Heim- oder kleinem Firmennetzwerk her oder richtet eine neue Verbindung ein.
Eine erweiterte Verbindung einrichten
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.
< Zurück
Weiter >
Abbrechen

Klicken Sie hier auf **Verbindung mit dem Netzwerk am Arbeitsplatz erstellen** und wählen im folgenden Fenster als **Netzwerkverbindung** die Option **VPN-Verbindung**. Im weiteren Verlauf geben Sie die **WAN IP-Adresse** des Routers an.

Folgen Sie nun den weiteren Anweisungen des Assistenten. Klicken Sie jeweils auf **Weiter**, um ins folgende oder auf **Zurück**, um ins vorherige Fenster zu gelangen.

Wenn Sie die Einrichtung der neuen Verbindung abgeschlossen haben, können Sie das **Startmenü** öffnen. Klicken Sie auf **Systemsteuerung** und wählen hier **Netzwerk- und Internetverbindungen**.

Im Bereich **Virtuelles privates Netzwerk** finden Sie jetzt ein Symbol für Ihre neue Verbindung, im Beispiel **VPN**.

Öffnen Sie die Verbindung durch Doppelklick auf das Symbol **VPN**.

In diesem Fenster geben Sie die Daten für die Verbindung ein.

Im Beispiel wird als Benutzername **VPN** und als Kennwort **1234** angegeben. Die Angaben müssen mit den Vorgaben im Nutzerprofil Ihres Teledat Routers übereinstimmen.

Besteht bereits eine Verbindung in das Internet, klicken Sie jetzt auf **Verbinden**, um die Verbindung zum Teledat Router aufzubauen.

Nach erfolgreichem Verbindungsaufbau befindet sich der entfernte Rechner im Netzwerk des Routers. Ist die Fernwartung aktiv, können Sie zum Beispiel durch Eingabe der IP-Adresse des Teledat Routers im Web-Browser dessen Konfigurationsmenü öffnen und Einstellungen vornehmen. Sie können jetzt ebenfalls auf die Rechner des lokalen Router-Netzwerkes zugreifen.

!

Beachten Sie, dass sämtliche Internetanfragen des eingewählten Rechners jetzt über den Teledat Router erfolgen.

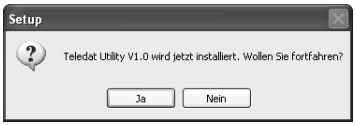
Anhang

Routertools für Microsoft Windows

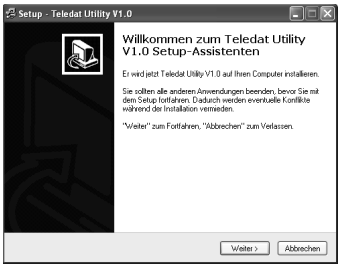
Installation der Routertools

Die mitgelieferten Routertools bieten Ihnen Unterstützung bei der Arbeit mit Ihrem Teledat Router. Das Utility **Teledat Firmware Upgrade** vereinfacht die Aktualisierung Ihrer Router Firmware. **Teledat Syslog** sammelt die SysLog Nachrichten des Teledat Routers und stellt diese anschaulich dar.

Installieren Sie bitte die Tools. Rufen Sie dazu auf der beigefügten CD-ROM aus dem Verzeichnis **Routertools** die Datei **TUSetup10.exe** auf. Die Beschreibung der Installation erfolgt beispielhaft am Betriebssystem Windows XP. Arbeiten Sie mit anderen Betriebssystemen (zum Beispiel Windows 98, Windows 2000) erfolgt die Installation ähnlich.



Klicken Sie in diesem Fenster auf **Ja**, um die Installation zu starten.


Setup - Teledat Utility V1.0
Willkommen zum Teledat Utility V1.0 Setup-Assistenten
Er wird jetzt Teledat Utility V1.0 auf Ihren Computer installieren.
Sie sollten alle anderen Anwendungen beenden, bevor Sie mit dem Setup fortfahren. Dadurch werden eventuelle Konflikte während der Installation vermieden.
"Weiter" zum Fortfahren, "Abbrechen" zum Verlassen.
Weiter >
Abbrechen

Es erscheint der Willkommensbildschirm des Installationsassistenten der Teledat Utilities.

Folgen Sie im weiteren Verlauf den Anweisungen dieses Assistenten. Klicken Sie jeweils auf **Weiter**, um die Installation fortzusetzen.

Setup - Teledat Utility V1.0
Setup Teledat Utility V1.0 abgeschlossen
Setup hat die Installation von Teledat Utility V1.0 auf Ihren Computer abgeschlossen. Die Anwendung kann über die installierten Programm-Verknüpfungen gestartet werden.
Klicken Sie auf "Fertigstellen", um das Setup zu beenden.
Fertigstellen

Beenden Sie die Installation durch Klicken auf **Fertigstellen**.

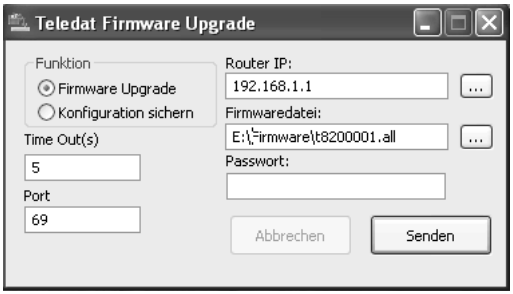
Sie können jetzt beide Utilities nutzen.

Teledat Firmware Upgrade

Das Utility **Teledat Firmware Upgrade** unterstützt Sie bei der Aktualisierung Ihrer Routerfirmware. Im Folgenden wird das Utility unter Windows XP vorgestellt.

Öffnen Sie jetzt das Utility **Teledat Firmware Upgrade.**

Klicken Sie auf **Start**. Führen Sie den Mauszeiger über **Programme**/**Teledat Utility** auf **Teledat Firmware Upgrade** und klicken Sie darauf.



Ein Fenster ähnlich dem nebenstehenden wird nun geöffnet.

Um ein Firmware Upgrade durchzuführen, muss in diesem Fenster die Funktion **Firmware Upgrade** aktiviert sein.

Tragen Sie unter **Router IP** die IP-Adresse Ihres Teledat Routers ein.

Im Feld **Firmwaredatei** geben Sie Verzeichnis und Namen der Upgrade-Datei an. Tragen Sie bei **Passwort** das Kennwort Ihres Teledat Routers ein. Klicken Sie auf **Senden**, um das Upgrade zu starten.

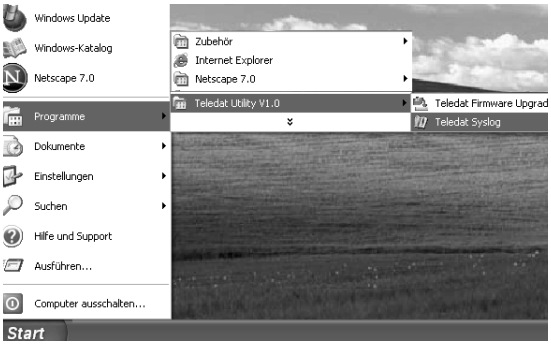
Nebenstehende Meldung erscheint, wenn das Upgrade erfolgreich durchgeführt wurde.

Erhalten Sie stattdessen eine Fehlermeldung, starten Sie Ihren Teledat Router bitte neu und wiederholen das Upgrade.

Teledat Syslog

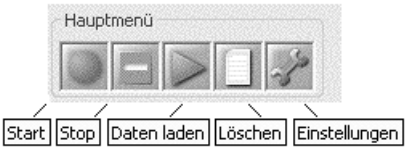
Das Utility **Teledat SysLog** sammelt die SysLog Nachrichten des Teledat Routers. Die Meldungen werden anschaulich dargestellt und können als Log-Datei gespeichert werden.

Im Folgenden wird das Utility unter Windows XP vorgestellt.

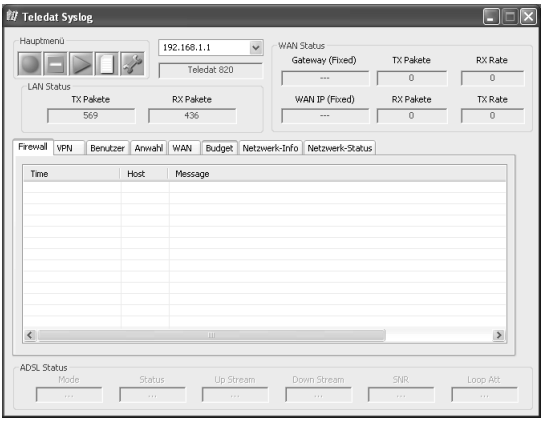


Öffnen Sie jetzt das Utility **Teledat Sys-Log.**

Klicken Sie auf **Start**. Führen Sie den Mauszeiger über **Programme**/**Teledat Utility** auf **Teledat SysLog** und klicken Sie darauf.



Nebenstehende Abbildung zeigt die **Funktionen**, die Sie über die Symbolleiste im Hauptmenü aufrufen können.



Starten Sie die Protokollfunktion, indem Sie auf das **Start**-Symbol klicken.

Die Bereiche **WAN**- beziehungsweise **LAN-Status** im oberen Bereich zeigen Informationen zu den aktuellen Netzwerkaktivitäten.

Die einzelnen **Register** enthalten die Angaben zu den verschiedenen SysLog-Bereichen, vorausgesetzt der jeweilige Bereich wurde über den Web-Konfigurator Ihres Teledat Routers aktiviert.

Bauen Sie nun zum Beispiel eine Internetverbindung auf, indem Sie mit Ihrem Browser eine Internetseite aufrufen. Anschließend sehen Sie unter dem Register **WAN** neue Informationen über die Internetverbindung (IP-Adresse und übertragene Pakete).

Mit einem Klick auf das Register **Anwahl** können Sie die gerade aufgebaute Internetverbindung aufgelistet sehen. Aus dem Protokoll ist ersichtlich, wann von welchem Rechner eine Internetverbindung gestartet wurde.

Öffnen Sie das Register **Benutzer** sehen Sie eine Übersicht aller Internetanfragen, die von Rechnern gestellt wurden.

Alle Listen werden ständig aktualisiert, bis mit der Taste **Stopp** die Aufzeichnung beendet wird.

Bitte beachten Sie, dass Sie mit dem Utility **Teledat Syslog** nur dann Informationen über den ADSL-Status erhalten können, wenn Sie es in Verbindung mit dem Teledat Router 830 verwenden, der über ein integriertes ADSL-Modem verfügt. Ein extern an den Teledat Router 800 angeschlossenes ADSL-Modem können Sie nicht mit dem Teledat Syslog Utility überwachen.

Erste Hilfe

Problem	Mögliche Ursache	Abhilfe
Auf der Vorderseite leuchtet keine LED.	Der Router ist ohne Strom, obwohl der Ein-/Ausschalter auf Ein steht.	Prüfen Sie, ob der Stecker des Netzteils richtig im Gerät sitzt. Prüfen Sie, ob die Steckdose in der das Netzteil steckt, Strom führt. Verwenden Sie dafür ein Gerät von dem Sie wissen, dass es funktioniert, zum Beispiel eine Schreibtischlampe.
Es leuchtet keine LED für das kabelgebundene LAN.	Der/die Stecker auf der Rückseite Ihres Routers sind nicht richtig eingesteckt.	Prüfen Sie den Sitz der Stecker, sowohl am Router als auch am Rechner.
Sie können nicht auf einen anderen Rechner im kabelgebundenen Netz oder WLAN zugreifen.	Die Rechner sind nicht auf automatische IP eingestellt, das heisst, sie sind nicht als DHCP-Clients konfiguriert.	Prüfen Sie die TCP/IP-Einstellungen der Rechner (siehe Seite 9). Prüfen Sie die Netzanbindung der Ethernetkarte des betreffenden Rechners (siehe Seite 9).
Sie erreichen mit dem Teledat Router keine Internetseiten, aber wenn Sie die IP-Adresse einer Seite eingeben, wird die Seite angezeigt.		Prüfen Sie zuerst die Angabe zur DNS-Adresse unter Netzwerkeinstellungen der betroffenen Rechner (siehe Seite 9). Besteht Ihr Problem weiterhin, prüfen Sie die Konfiguration Ihres Routers bezüglich der DNS-Konfiguration (siehe Seite 20).
Login in den Router schlägt fehl.	Passwort wurde vergessen.	In diesem Fall hilft leider nur ein Reset des Routers. Dadurch wird er auf die Werkseinstellungen zurückgesetzt (siehe Seite 58). Das Passwort lautet danach wieder **1234**.

Problem	Mögliche Ursache	Abhilfe
Schwierigkeiten mit der T-Online-Kennung.	Benutzername ist nicht korrekt angegeben.	Achten Sie auf korrekte Angabe der Benutzerkennung: »Anschlusskennung« + »T-Online Nummer« + »#« + »Mitbenutzernummer« + »@t-online.de« Sollte die T-Online Nummer 12 Zeichen lang sein, muss eventuell die Raute (#) weggelassen werden. Zusammensetzung des Benutzernamen beim Business-Tarif: »t-online-com/« + »Benutzerkennung« + »@t-online-com.de«

Service / Support

Bei technischen Problemen mit Ihrem Teledat Router können Sie sich während der üblichen Geschäftszeiten an die T-Service Hotline 0180 5 1990 wenden. Der Verbindungspreis beträgt 0,12 EUR pro angefangene 60 Sekunden bei einem Anruf aus dem Festnetz der Deutschen Telekom (Stand Mai/2003). Erfahrene Techniker beraten Sie auch bei der Bedienung Ihres T-Com-Gerätes.

CE-Zeichen

Diese Gerät erfüllt die Anforderungen der EU-Richtlinie:

1999/5/EG Richtlinie über Funkanlagen und Telekommunikationseinrichtungen und die gegenseitige Anerkennung ihrer Konformität.

Die Konformität mit der oben angegebenen Richtlinie wird durch das CE-Zeichen auf dem Gerät bestätigt.

Die Konformitätserklärung kann unter folgender Adresse eingesehen werden:

Deutsche Telekom AG
Geschäftsbereich Endgeräte
CE-Testlab Steinfurt
Sonnenschein 38
48565 Steinfurt

Technische Daten

Leistungsmerkmale

- Ethernet-WAN-Port mit 10 Mbit/s
- Ethernet-Vierfach-Switch 10/100 Mbit/s, autosensing, Auto-MDI/MDI-X, RJ45
- Konfiguration über Web-Browser
- Automatische Zeit- und Datumseinstellung
- Kostenkontrolle durch einstellbare Online-zeit- und Datenvolumen-Budgets
- Online-LED leuchtet, wenn eine gebühren-pflichtige Verbindung besteht

Sicherheit

- Passwortgeschützte Router-Einstellungen
- Firewall mit IP-Packetfilterung und Stateful Inspection
- Erkennt und schützt vor DoS-Angriffen
- Reagiert nicht auf Pings am WAN-Port

VPN-Funktionalitäten

- Bis zu 8 gleichzeitige VPN-Verbindungen (Client- und Serverbetrieb)
- Tunnelprotokolle: PPTP, L2TP und IPSec
- IPSec-Verschlüsselung mit DES oder 3DES
- VPN Pass Through (PPTP / L2TP)
- Dynamische LAN-LAN-Kopplung

Unterstützte Protokolle

- NAT mit Portumleitung, Portfreischaltung und DMZ
- DHCP-Client und Server (abschaltbar)
- DNS mit Cache und Proxy
- PPPoE mit automatischem oder manuellem Verbindungsaufbau
- PAP und CHAP zur Authentifizierung
- Dynamisches DNS
- Statische Routen
- SysLog-Unterstützung (Tool auf CD)
- Fernwartung (einschaltbar)

Systemvoraussetzungen

- T-DSL-Anschluss und T-DSL-Modem
- Rechner mit RJ45-Ethernetanschluss und TCP/IP-Unterstützung

Betriebssysteme für ISDN-Software und Teledat Router-Tools

- Windows 98/ME
- Windows 2000
- Windows XP
- Die Konfiguration des Teledat Routers 800 erfolgt betriebssystemunabhängig per Web-Browser.

Abmessungen

- B/H/T (in cm): 20,1 x H 16,7 x T 3,6

Gewicht

430 Gramm

Stromversorgung

- 230V Euro-Netzteil

Betriebsbedingungen

- Temperatur: 0 bis 50 °C
- relative Luftfeuchte (nicht kondensierend): 10 % - 90 %

Gewährleistung

Der Händler, bei dem das Gerät erworben wurde (Deutsche Telekom oder Fachhändler), leistet für Material und Herstellung des Telekommunikationsendgerätes eine Gewährleistung von 2 Jahren ab der Übergabe.

Dem Käufer steht im Mangelfall zunächst nur das Recht auf Nacherfüllung zu. Die Nacherfüllung beinhaltet entweder die Nachbesserung oder die Lieferung eines Ersatzproduktes. Ausgetauschte Geräte oder Teile gehen in das Eigentum des Fachhändlers über.

Bei Fehlschlagen der Nacherfüllung kann der Käufer entweder Minderung des Kaufpreises verlangen oder von dem Vertrag zurücktreten und, sofern der Mangel von dem Händler zu vertreten ist, Schadensersatz oder Ersatz vergeblicher Aufwendungen verlangen.

Der Käufer hat festgestellte Mängel dem Händler unverzüglich mitzuteilen. Der Nachweis des Gewährleistungsanspruchs ist durch eine ordnungsgemäße Kaufbestätigung (Kaufbeleg, ggf. Rechnung) zu erbringen.

Schäden, die durch unsachgemäße Behandlung, Bedienung, Aufbewahrung, sowie durch höhere Gewalt oder sonstige äußere Einflüsse entstehen, fallen nicht unter die Gewährleistung, ferner nicht der Verbrauch von Verbrauchsgütern, wie z. B. Druckerpatronen, und wiederaufladbaren Akkumulatoren.

Vermuten Sie einen Gewährleistungsfall mit Ihrem Telekommunikationsendgerät, können Sie sich während der üblichen Geschäftszeiten an die T-Service Hotline 0180 5 1990 wenden. Der Verbindungspreis beträgt 0,12 EUR pro angefangene 60 Sekunden bei einem Anruf aus dem Festnetz der Deutschen Telekom (Stand 05/2003). Erfahrene Techniker beraten Sie und stimmen mit Ihnen das weitere Vorgehen ab.

Reinigen

Wischen Sie den Teledat Router von Zeit zu Zeit mit einem leicht feuchten, fusselfreien Tuch oder mit einem Antistatiktuch ab, niemals mit einem trockenen Tuch (wegen statischer Aufladung).

Vermeiden Sie bitte den Einsatz von aggressiven Putz- und Scheuermitteln.

Recycling

Hat Ihr Teledat Router ausgedient, nimmt die Deutsche Telekom von ihr gemietete oder bei ihr gekaufte Geräte in den T-Punkten kostenlos zurück. Die Deutsche Telekom zerlegt die Endgeräte fachgerecht und führt sie dem Recycling zu.

Tipp

Wollen Sie das Gerät zum Beispiel zur Reparatur geben, führen Sie ein Reset aus (siehe Seite 62), um Ihre Einstellungen zu löschen und deren Mißbrauch zu verhindern.

A

Adresstabelle-NAT..... 66
Aktualisierung Firmware..... 60
Anbindung Netzwerkkarte.....9
Anschlüsse.....8
Anwahlpaket..... 63
Anzeigen.....III
ARP-Cache..... 65
Assistent.....18
Aufstellungsort..... 7

B

Basiskonfiguration..... 18
Betriebssysteme..... 10
Benutzerkennung.....22
Benutzerprofil 44
Benutzereinwahl
- VPN.....80
Bidirektionale Kopplung
- VPN.....71
Broadcast..... 36
Browser..... 12
Budgetkontrolle.....27

C

CE-Zeichen.....88

D

Datenfilter..... 31
DDNS.....54
DHCP-Server..... 20
Diagnose.....62
DMZ..... 42
DNS.....20
DoS-Abwehr..... 35
DSL-Anschluss..... 8
DSL-Modem..... 24
Dynamisches DNS..... 54

E

Eigenschaften TCP/IP.....9
Einwahleinstellungen..... 43
Einwahlfilter.....31
Entfernte Nutzer.....44
Erstkonfiguration.....15
Erste Hilfe..... 86
Ethernetkarte..... 9
Externe Einwahl.....80

F

Fernwartung 57
Filterregel.....33
Firewall.....31
Firmware..... 60
Fragmentierung.....31

G

Gateway 20
Gesamtansicht..... III
Gesamtbudget.....28

H

Hardwareinstallation.....8

I

Installieren - Routertools..... 82
Internet-Timeserver..... 19
Internetzugang..... 22
IP-Adresse..... 20
IP-Filter..... 32
IP-Netzwerkkonfiguration..... 20
IP-Sec
- Tunnel..... 48
- Schlüssel..... 51
ISP..... 22

K

Kennwort..... 16
Konto..... 27

L

LAN
- Anschluss..... 9
- einbinden ins..... 9
LAN-LAN-Kopplung..... 67
Leerlaufzeit..... 22
Leistungsmerkmale..... 90
Leuchtdioden..... III
Lieferumfang..... 6
Logfile..... 58
Login..... 16

M

MAC-Adresse..... 26

N

NAT..... 31
Netzwerkkonfiguration..... 20
Neustart..... 62

O

Öffentliche IP..... 17
Onlinekonto..... 27
Originalverpackung..... 6

P

Passwort 16
Ping..... 57
Port..... 37
Portöffnung..... 40
Portumleitung..... 37
PPPoE..... 22
PPTP..... 24
Protokollrechner..... 58

R

Reinigen..... 91
Recycling..... 91
Routerkonfiguration..... 16
Routertools..... 82
Routingtabelle..... 64

S

Schlüssel..... 51
Serviceline..... 88
Sicherheitshinweise..... II
Sichern..... 59
Startadresse..... 45
Stateful Inspection..... 34
Static Route..... 53
Status
- DSL..... 17

Stromnetz..... 8
SysLog.....58
Systemvoraussetzungen.....7
Systemzeit..... 19

T

TCP/IP, Eigenschaften.....9
Technische Daten..... 89
Teledat Firmware Upgrade.....83
Teledat SysLog.....84
Timeserver.....19

U

Unidirektionale Kopplung
- VPN.....67
Unterlagen Dienstanbieter.....22
Upgrade.....60
URL 54

V

Verbindungstimer.....56
Verpackungsinhalt.....6
Verschlüsselungsmethode.....53
Verwaltung..... 57
Virtuelles Netz..... 43
VPN.....43
VPN Pass Through.....43

W

WAN..... 8
Wandmontage..... 7
Warenzeichen..... 88
Warngrenze.....27
Web-Konfigurator..... 12
Werkseinstellungen..... 62
Wiederherstellen..... 59
Windows..... 10

Z

Zeitkonto.....27
Zugangskontrolle..... 43
Zugriffskontrolle..... 57

3DES Der **Dreifach-DES**-Schlüssel ist eine Mehrfachverschlüsselung auf Basis des DES (siehe unten). Der symmetrische Verschlüsselungsalgorithmus 3DES benutzt zwei Schlüssel (oder drei) und drei DES-Durchläufe.

AH **A**uthentication **H**eader ist ein integraler Bestandteil von IPsec. Er ist ein Protokoll zur Sicherstellung von Authentität und Integrität eines IP-Paketes in einem virtuellen privaten Netzwerk.

ARP Das **A**ddress **R**esolution **P**rotocol dient zur Adreßauflösung. Die Aufgabe besteht darin, zu einer gegebenen Protokoll-Adresse die zugehörige Netzwerk-Hardware-Adresse (MAC-Adresse) herauszufinden.

BOD **B**andwidth **O**n **D**emand ist das dynamische An- und Ausschalten des zweiten B-Kanals eines Basisanschlusses des ISDN bei Bedarf. Wird bei der Datenübertragung die Datenrate für eine einstellbare Dauer übertroffen, wird automatisch der zweite hinzugeschalten. Sinkt die Datenrate wieder unter einen unteren Wert, wird der zweite B-Kanal wieder freigegeben. Größere Downloads werden dadurch automatisch mit der maximal erreichbaren Geschwindigkeit von ca. 15 KB durchgeführt, während des Surfens wird nur ein B-Kanal benutzt.

CBCP **C**all **B**ack **C**onfiguration **P**rotocol: nach der ersten Kontaktaufnahme erfolgt Rückruf unter einer bestimmten Telefonnummer.

CHAP **C**hallange **H**andshake **A**uthentication **P**rotokol ist ein Verfahren zur Authentifizierung bei PPP.

DES Der **D**ata **E**ncryption **S**tandard ist ein kryptographischer Algorithmus für die Verschlüsselung und Entschlüsselung von Daten.

DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol ist ein Protokoll zur dynamischen Vergabe von IP-Adressen. Dabei schöpft der DHCP-Server aus einem vorgegebenen Adressenbereich und weist den anfragenden Clients eine Adresse für einen bestimmten Zeitraum zu.

DMZ **D**e**M**ilitarized **Z**one ist eine Firewall-Technik zum Schutz eigener Netzwerke gegenüber öffentlich zugänglichen Netzen. Die im DMZ befindlichen Server gehören strategisch nicht zum internen Unternehmensnetz und können daher auch keine Informationen aus diesem weiterreichen. In der DMZ sind üblicherweise Web-, und Mail-Server untergebracht.

DNS **D**omain **N**ame **S**ystem ist ein Adressierungssystem im Internet, das in der Lage ist, von Menschen lesbare Maschinennamen in IP-Adressen umzusetzen, beispielsweise www.Mustermann.info in die IP-Adresse 192.66.46.2.

DDNS **D**ynamischer **DNS** ist die Verknüpfung einer festen URL mit der jeweils aktuellen IP-Adresse.

DoS **D**enial **o**f **S**ervice sind Attacken im Internet zur Beeinträchtigung von Diensten, die damit außer Betrieb gesetzt werden. DoS-Attacken zielen in der Regel nicht auf den Zugang zum Netzwerk, zu einem bestimmten System oder zu den Datenbeständen ab, sondern haben das Ziel einen Dienst einzuschränken, zu blockieren oder unbenutzbar zu machen. Dazu werden die zur Verfügung stehenden Programme oder Netzwerk-Ressourcen außerordentlich überbelastet.

ESP **E**ncapsulating **S**ecurity **P**ayload ist ein Protokoll zur Verschlüsselung eines Datenpaketes und zur Integritätssicherung.

IKE **I**nternet **K**ey **E**xchange dient der Verständigung über die zu verwendenden Sicherheitsalgorithmen und dem dazu notwendigen Austausch von Schlüsselmaterial.

IP **I**nternet **P**rotokoll ist die Grundlage der Protokollfamilie TCP/IP und für die Weiterleitung der Daten zuständig.

IPCP **I**nternet **P**rotocol **C**ontrol **P**rotocol ist ein NCP-Protokoll zur Übertragung des IP-Protokolls mittels PPP-Protokoll.

IPSec **I**nternet **P**rotocol **Sec**urity ist ein Standard, bei dem die Datagramme des LAN beim Übergang zum Internet verschlüsselt werden.

ISP **I**nternet **S**ervice **P**rovider ist ein Anbieter von Internet-Diensten, zum Beispiel T-Online.

L2TP **L**ayer Two(**2**) **T**unneling **P**rotocol wird zur Benutzerauthentifizierung im Rahmen der Datenübertragung eingesetzt.

LAN **L**ocal **A**rea **N**etwork ist ein lokales Netzwerk.

LED **L**ight **E**mitting **D**iode ist eine Leuchtdiode zur Statusanzeige.

MSN **M**ulti **S**ubscriber **N**um sind die Mehrfachrufnummern bei einem Euro-ISDN-Anschluss (in der Regel drei) für Zuweisung an verschiedene Endgeräte (zum Beispiel Telefon, Fax, Rechner).

NAT **N**etwork **A**dress **T**ranslation ermöglicht es mehreren Clients in einem Netzwerk die gleiche externe IP-Adresse zu benutzen. Diese erscheint gegenüber anderen Servern als Ursprungsadresse. Die Clients sind so gegen direkte Angriffe aus dem Internet geschützt. Die Zuordnung interne - externe IP wird in einer NAT-Tabelle aufgezeichnet. Dadurch ist es möglich, dass die Antwort des Servers auch an den richtigen Client im internen Netzwerk gesendet wird.

NCP **N**etWare **C**ore **P**rotocol ist ein spezifisches Protokoll für die Kommunikation in Client-Server-Architekturen.

NTBA	**N**etwork **T**ermination for **B**asic **A**ccess ist das Netzabschlußgerät (die Netzterminierung) eines ISDN Basisanschlusses.
PAP	**P**assword **A**uthentication **P**rotokoll ist ein Verfahren zur Authentifiziereung bei PPP.
PPTP	**P**oint-to-**P**oint **T**unneling **P**rotocol ist ein Punkt-zu-Punkt Tunneling Protokoll, das eine geschützte Verbindung (durch Verschlüsselung der Daten) innerhalb einer Internet-Verbindung erzeugt.
PPP	Das **P**oint-to-**P**oint **P**rotokoll ist ein Verbindungsprotokoll für Punkt zu Punkt Kommunikation.
PPPoE	**PPP o**ver **E**thernet Protocol ist das verwendete Protokoll bei einer ADSL-Verbindung zum Internet.
RIP	**R**outer **I**nformation **P**rotocol ist das zu Grunde liegende Protokoll für Routing. Bei RIP schicken alle Router in Intervallen ihre eigenen Routing-Tabellen als Broadcast an die anderen Router. RIP gibt es in zwei Versionen: die Version 2 von RIP, RIPv2, baut auf dem Distance-Vector-Algorithmus auf und benutzt wie RIPv1 das UDP-Protokoll für den Transport der Routing-Tabellen.
TCP	**T**ransport **C**ontrol **P**rotocol ist ein verbindungsorientiertes End-to-End -Protokoll zwischen verschiedenen Netzwerken.
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol ist ein einfaches File-Transfer-Protokoll, das von den TCP/IP-Protokollen unterstützt wird.
UDP	**U**ser **D**atagram **P**rotocol ist eine um die Transportsicherung erleichtete Version des TCP.
URL	**U**niform **R**esource **L**ocator ist eine Adresse, die den genauen Ort einer Ressource im Internet angibt.
VPN	Ein **V**irtuelles **P**rivates **N**etzwerk verbindet zwei Netzwerke, einen Compututer mit einem Netzwerk oder zwei Computer über öffentliche Verbindungen wie zum Beispiel das Internet. Kommunikationsgrundlage eines IP-basierten VPNs ist das PPP-Protokoll mit IP-Tunneling.
VTA	**V**irtual **T**erminal **A**dapter ist eine technische Einrichtung für den Anschluss von Endeinrichtungen an den Basisanschluss (ISDN-Adapter). Mit Hilfe von Terminal-Adaptern können Endgeräte oder Zusatzeinrichtungen ohne ISDN-Schnittstelle an ISDN angeschlossen werden.
WAN	**W**ide **A**rea **N**etwork ist ein Computernetzwerk, das sich über eine größere räumliche Fläche erstreckt.

CE

Herausgeber:

Deutsche Telekom AG
T-Com
Postfach 2000
53105 Bonn

MNr.: 40204437
Stand: November 2003